

#2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of : Naoki OGUCHI
Filed: : Concurrently herewith
For: : PACKET RELAYING APPARATUS AND....
Serial No. : Concurrently herewith

11017 U.S. PTO
10/090862
03/05/02

Assistant Commissioner for Patents
Washington, D.C. 20231

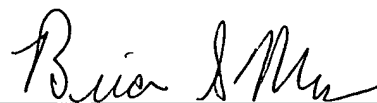
March 5, 2002

PRIORITY CLAIM AND SUBMISSION
OF PRIORITY DOCUMENT

S I R:

Applicant hereby claims priority under 35 USC 119 from JAPANESE patent application no. 2001-062685 filed March 6, 2001, a certified copy of which is enclosed.

Respectfully submitted,



Brian S. Myers
Reg. No. 46,947

ROSENMAN & COLIN, LLP
575 MADISON AVENUE
IP Department
NEW YORK, NEW YORK 10022-2584
DOCKET NO.: FUJ 19.011
TELEPHONE: (212) 940-8800

日 本 国 特 許 庁
JAPAN PATENT OFFICE



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 3月 6日

出 願 番 号

Application Number:

特願2001-062685

出 願 人

Applicant(s):

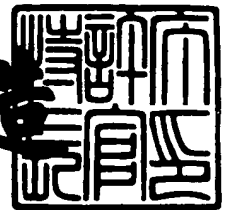
富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 8月31日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出 証 番 号 出 証 特 2001-3080882

【書類名】 特許願

【整理番号】 0052258

【提出日】 平成13年 3月 6日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/56

【発明の名称】 パケット中継装置およびパケット中継方法

【請求項の数】 5

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 小口 直樹

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100108187

【弁理士】

【氏名又は名称】 横山 淳一

【電話番号】 044-754-3035

【手数料の表示】

【予納台帳番号】 011280

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0017694

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 パケット中継装置およびパケット中継方法

【特許請求の範囲】

【請求項 1】 入力されたパケットに対応する送信元仮想閉域網識別子に基づき、該パケットの中継が許されている 1 つ以上の仮想閉域網を選択する手段と

前記 1 つ以上の仮想閉域網に対応する 1 つ以上の経路ドメインを選択する手段と、

前記パケットの送信先アドレスと前記 1 つ以上の経路ドメインの各経路ドメイン情報とを照合し、前記パケットを次のパケット中継装置に送出するための送出アドレスを選択する手段と、

前記送出アドレスに前記パケットを送出する手段を有することを特徴とするパケット中継装置。

【請求項 2】 入力されたパケットの送信元仮想閉域網識別子に基づき、該パケットの中継が許されている 1 つ以上の仮想閉域網を選択するステップと、

前記 1 つ以上の仮想閉域網に対応する 1 つ以上の経路ドメインを選択するステップと、

前記パケットの送信先アドレスと前記 1 つ以上の経路ドメインの各経路情報とを照合し、前記パケットの送出先アドレスを選択するステップと、

前記送出先アドレスに前記パケットを送出するステップを有することを特徴とするパケット中継方法。

【請求項 3】 複数の送信元仮想閉域網識別子と該各送信元仮想閉域網識別子に対応する 1 つ以上の宛先仮想閉域網識別子を管理するポリシ管理部と、

前記ポリシ管理部から 1 つ以上の送信元仮想閉域網識別子と該 1 つ以上の各送信元仮想閉域網識別子に対応する 1 つ以上の宛先仮想閉域網識別子を該 1 つ以上の各送信元仮想閉域網識別子に対応させて端末に表示する表示部と

を備えることを特徴とするパケット中継装置。

【請求項 4】 各宛先仮想閉域網識別子と該各宛先仮想閉域網識別子に対応する 1 つ以上の経路ドメイン識別子を管理する仮想閉域網管理部を備え、

前記仮想閉域網管理部は端末から入力される1つの宛先仮想閉域網識別子と該1つの宛先仮想閉域網識別子に対応する1つ以上の経路ドメイン識別子に対応させて前記端末に表示する表示部と

を備えることを特徴とするパケット中継装置。

【請求項5】 端末からの指示に基づきドメイン間中継ポリシーテーブルに設定された各送信先仮想閉域網識別子および前記各送信先仮想閉域網識別子に対応する経路ドメインの一覧を要求する手段と、

前記要求に基づいてドメイン間中継ポリシーテーブルから1つ以上の送信先仮想閉域網識別子を抽出し、前記各送信先仮想閉域網識別子に対応する経路ドメインの一覧を抽出する手段と、

抽出された前記各送信先仮想閉域網識別子および前記各送信先仮想閉域網識別子に対応する経路ドメインの一覧を前記端末に表示する手段を備えることを特徴とするパケット中継装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、通信サービスを提供するパケット中継装置及びパケット中継方法に関し、特に、仮想閉域網（Virtual Private Network）間及び経路ドメイン間でのパケットの中継に関するパケット中継装置及びそのパケット中継方法に関する。なお、以下、経路ドメインをドメインと呼ぶことがある。

【0002】

【従来技術】

近年、インターネットの普及により、ユーザ（例えば、企業や大学など）ではATM（Asynchronous Transfer Mode）やFR（Frame Relay）などによる仮想専用線（Virtual Path/Virtual Channel）を利用しなくとも、分散する各拠点間はインターネットを介して通信できるようになった。この通信ではVPNを構築することがある。以降、VPNを仮想閉域網と呼ぶことがある。

【0003】

そして、ユーザのネットワーク内に限ってIPアドレスを独自に割り当て、運用するユーザが現れてきている。このようなユーザのネットワーク内でプライベートのIPアドレスを使用した場合、そのプライベートIPアドレスを有するパケットをそのままグローバルのIPアドレスを持つインターネットに流すことはできない。

【0004】

プライベートのIPアドレスとグローバルのIPアドレスがインターネット上で重複して使用されることになり、インターネットを介した通信を正常に行うことができない可能性が生じるためである。

【0005】

したがって、このようなユーザのプライベートネットワークの各拠点間でインターネットを経由して通信を行うときには、このユーザ内のプライベートネットワークからインターネットへの接続では、例えば、グローバルIPアドレスを持つIPパケットでカプセル化（トンネリング化）してインターネットに転送し、受信側拠点のインターネット網接続ルータでカプセル化されたこのパケットを受信すると同時にカプセル化を解き、受信側の拠点内の宛先ホストにルーティングするといった仕組みが必要となる。

【0006】

この場合、ユーザは、プライベートのIPアドレスを有するIPパケットをグローバルIPアドレスによりトンネル（送信側ではカプセル化、受信側ではデカプセル化）する装置を備える必要がある。すなわち新たな機器の導入が生じる。

【0007】

また、カプセル化、デカプセル化する処理が新たに必要となるため性能が低下する可能性もある。なお、以下の記述において中継装置をルータと記述することがある。

【0008】

さらに、ユーザにおいて、各拠点をそれぞれインターネットに接続する際、各拠点のルータにおいて、経路制御および論理インタフェース等の設定は、各拠点

間の設定の組み合わせ数が増加するにつれてより複雑になる。この場合、ネットワーク機器の導入・維持管理およびネットワーク管理者の育成にコストがかかるという問題がある。

【0009】

そこで、ユーザがインターネットを介して各拠点間を通信するVPNを導入する場合、そのVPNの導入・維持管理をプロバイダ（本発明ではキャリアを含む）にアウトソース（委託）することにより、ユーザは既存のネットワークにほとんど手を加えることなしにVPNサービスの提供を受けることができる。

【0010】

このVPNサービスでは、トンネルの始終端機能をプロバイダのルータで実現する。そして、あるユーザが複数の拠点を持っている場合、プロバイダのルータは送信元のユーザ拠点から受信したIPパケットをどの宛先ユーザ拠点のネットワークにカプセル化して送信すべきか決定する経路制御機能を備えている。

【0011】

この機能は、アウトソースによりプロバイダのルータが提供する。このようにプロバイダによりVPNサービスが行われ場合、プロバイダのエッジルータでは、インターネット網の経路制御機能とは別にユーザネットワーク固有の経路制御機能によりIPパケットが転送される。

【0012】

したがって、プロバイダが提供するVPNサービスは、各ユーザの各拠点ネットワークごとに経路制御機能を独立に管理する必要性があることからその設定が非常に複雑になる。

【0013】

ユーザがVPNを構築することもあるが、ここではプロバイダがVPNを構築しユーザにVPNサービスを提供することを前提に説明する。ネットワークを管理する主体の観点から分類すると、複数拠点の管理主体が同一であるネットワークを「イントラネット（Intranet）」と呼び、例えば、管理主体が同一企業により運用されるネットワークを示す。

【0014】

また複数拠点の管理主体が同一でないネットワークを「エクストラネット (Extranet)」と呼び、例えば、異なる独立した企業により運用されるネットワークを示す。また、イントラネットおよびエクストラネットのそれぞれがどのような経路ドメインから構成されているかといった観点からも分類することができる。

【0015】

すなわち、1つのネットワークが単一の経路ドメインから構成されている場合をシングルドメインと呼び、複数の経路ドメインから構成されている場合をマルチドメインと呼ぶ。このように、シングルドメイン／マルチドメイン、イントラネット／エクストラネットの組み合わせによるネットワーク構成の例を図1に示す。なお、全図をとおして同じ参照符号は同一物または同等物を示す。

【0016】

しかしながら、一般的にはイントラネットにおいて一つの管理主体が管理するネットワーク内で複数の経路ドメインが存在することは少ないので、本明細書では、以下単にイントラネットといった場合は、シングルドメインのイントラネットを示すものとする。

【0017】

また、エクストラネットにおいては、複数の管理主体が管理するそれぞれのネットワークで異なる中継ルール (ポリシー) を持っていることが多いと考えられるため、以下単にエクストラネットと呼ぶ場合は、マルチドメインのエクストラネットを示すものとする。

【0018】

次に、図2および図3は、前述の図1に示すシングルドメイン、マルチドメイン構成のVPNを収容するルータがどのように中継テーブルを構成するかを説明している。

ー 第1の従来技術

図2はプロバイダを介して接続されるシングルドメイン構成のイントラネットVPNを収容するルータの中継テーブルの構成例を説明する図である。

【0019】

図中、パケット受信部113はドメイン識別テーブル109を参照し、入力されたパケットの送信元経路ドメインを識別する。そして、そのパケットがルーティングパケットである場合は、イントラネットドメイン経路情報処理部101に送出される。

【0020】

例えば、図示していない経路ドメイン#11からのルーティングパケットである場合には、イントラネットドメイン経路情報管理部102（図中、左側）では、そのルーティングパケットを受信し、各VPNに対応して設けられたVPN#11に対応するイントラネットドメイン中継テーブル104（図中、左側）に書き込む。すなわち、経路ドメイン#11からのパケットは経路ドメイン#11のみに中継することができる。

【0021】

一方、図示していない経路ドメイン#12に対応するイントラネットドメイン経路情報管理部102（図中、右側）はVPN#11及びVPN#12のイントラネットドメイン中継テーブル104（図中、左及び右側）に書き込みを行う。すなわち、経路ドメイン#12からのパケットは、経路ドメイン#11及び経路ドメイン#12の両方に中継することができる。このように経路ドメイン#11及び経路ドメイン#12との間の接続性可否の処理をイントラネットドメイン経路情報管理部102と対応するイントラネットドメイン中継テーブル104との連携により処理していた。

【0022】

パケット中継部111はパケット受信部113からパケットを受信した場合には、送信先IPアドレスに基づき各VPNに対応する各イントラネットドメイン中継テーブル104を順次検索し、該パケットを転送すべき次ホップルータのIPアドレスを求める。

【0023】

そして、パケット送信部112の出力インタフェース情報とともに送信先の該IPアドレスを有するパケットをパケット送信部112に送出する。パケット送信部112は指示された出力インタフェースを選択し、該パケットを送出する。

なお、送信先IPアドレスが各VPNに対応するイントラネットドメイン中継テーブル104に存在しなかった場合、そのパケットは破棄される。

【0024】

各イントラネットドメイン中継テーブル104は、送信先IPアドレス、IPアドレスマスク情報、出力インターフェイス情報、次ホップルータIPアドレス等を含むように構成する。

【0025】

また、定期的に、イントラネットドメイン経路情報処理部101が保有する経路ドメイン情報をルーティングパケットに含めてパケット送信部112に送出し、パケット送信部112は該ルーティングパケットを隣接のルータに配布する。

ー 第2の従来技術

図3はマルチドメイン構成のエキストラネットVPNを収容するルータの中継テーブルの構成例を説明する図である。図2と図3との本質的な相違点は、イントラネットからエキストラネットに対応できるように変更されていること、およびドメイン定義部105Aとエキストラネット間中継ポリシ107Aを新たに設けた点である。この相違点に着目し、説明する。

【0026】

図中、エキストラネットドメイン経路情報処理部101Aのエキストラネットドメイン経路情報管理部102Aは、通常、ルータが管理している経路ドメインの数だけ存在する。送信元の経路ドメインに対応するエキストラネットドメイン経路情報管理部102Aはルーティングパケットを受信し、そのパケットの送信元の経路ドメインに対応するエキストラネットドメイン中継テーブル104Aにルーティング情報を書き込む。

【0027】

パケット中継部111はパケット受信部113からパケットを受信した場合に、そのパケットの送信元の経路ドメイン情報に対応するエキストラネットドメイン中継ポリシ107Aを検索し、該パケットを中継できる経路ドメインの一覧を検索する。そして、取得した経路ドメインの一覧および送信先IPアドレスをパラメタにしてドメイン定義部105Aを呼び出す。

【 0 0 2 8 】

ドメイン定義部 1 0 5 A はパラメタとして与えられた経路ドメインの一覧から順次経路ドメインを取り出し、送信先 I P アドレスを用いて該経路ドメインに対応するエクストラネットドメイン中継テーブル 1 0 4 A を検索し、該パケットを転送すべき次ホップルータの I P アドレスを求める。

【 0 0 2 9 】

そして、パケット送信部 1 1 2 の出力インタフェース情報とともに送信先の該 I P アドレスを有するパケットをパケット送信部 1 1 2 に送出する。パケット送信部 1 1 2 は指示された出力インタフェースを選択し、該パケットを送出する。

【 0 0 3 0 】

このようにパケットの中継処理では、ある送信元のイントラネット V P N やエクストラネット V P N から送信先 V P N となる他のエクストラネットやマルチドメインで構成されるイントラネットへの中継ポリシーを定義したい場合、次の課題がある。

【 0 0 3 1 】

【発明が解決しようとする課題】

第 1 の従来技術に示した構成では、各送信元経路ドメインに対する各 V P N 中継テーブルに送信先 V P N に対応する経路情報を書き込む。このため、同じ送信先 V P N に対し複数の送信元 V P N が接続性を定義しようとした場合、複数の送信元 V P N に対する中継テーブルに同じ送信先 V P N の経路情報がコピーされ、全体としてメモリを多く消費する。

【 0 0 3 2 】

第 2 の従来技術に示した構成では、送信元 V P N を構成するドメインと、送信先 V P N の複数のドメイン間との全ての組み合わせに対し中継ポリシーを個別に定義する必要がある、中継ポリシーの設定／変更が複雑である。

【 0 0 3 3 】

以上から本発明の第 1 の課題は、中継ポリシーの設定／変更を容易にすることであり、また、本発明の第 2 の課題は、中継装置で使用されるメモリの使用量の削減することとし、第 1 及び第 2 の課題のうち、少なくとも 1 つの課題を解決するこ

とを目的とする。

【0034】

【課題を解決するための手段】

本発明は、上述した課題を解決するために以下の構成をとる。

本発明のパケット中継装置は、入力されたパケットに対応する送信元仮想閉域網識別子に基づき、該パケットの中継が許されている1つ以上の仮想閉域網を選択する手段と、前記1つ以上の仮想閉域網に対応する1つ以上の経路ドメインを選択する手段と、前記パケットの送信先アドレスと前記1つ以上の経路ドメインの各経路ドメイン情報とを照合して前記パケットを次のパケット中継装置に送出するための送出先アドレス（次ポップルータアドレス）を選択する手段と、前記送出先アドレスに前記パケットを送出する手段を有することを特徴とする。

【0035】

また、本発明のパケット中継方法は、入力されたパケットの送信元仮想閉域網識別子に基づき、該パケットの中継が許されている1つ以上の仮想閉域網を選択するステップと、前記1つ以上の仮想閉域網に対応する1つ以上の経路ドメインを選択するステップと、前記パケットの送信先アドレスと前記1つ以上の経路ドメインの各経路情報（destination）とを照合し、前記パケットの送出先アドレス（次ポップルータアドレス）を選択するステップと、前記送出先アドレスに前記パケットを送出するステップを有することを特徴とする。

【0036】

また、本発明のパケット中継装置は、複数の送信元VPN識別子（送信元仮想閉域網識別子）と該各送信元VPN識別子に対応する1つ以上の宛先VPN識別子（宛先仮想閉域網識別子）を管理するポリシ管理部（VPN間中継ポリシ実施部）と、前記ポリシ管理部から1つ以上の送信元VPN識別子（送信元仮想閉域網識別子）と該1つ以上の各送信元VPN識別子（送信元仮想閉域網識別子）に対応する1つ以上の宛先VPN識別子（宛先仮想閉域網識別子）を該1つ以上の各送信元VPN識別子（送信元仮想閉域網識別子）に対応させて端末に表示する表示部（構成情報設定表示部）とを備えることを特徴とする。

【0037】

また、本発明のパケット中継装置は、各宛先VPN識別子（宛先仮想閉域網識別子）と該各宛先VPN識別子に対応する1つ以上の経路ドメイン識別子を管理する仮想閉域網管理部（VPN定義部）を備え、前記仮想閉域網管理部は端末から入力される1つの宛先VPN識別子と該1つの宛先VPN識別子に対応する1つ以上の経路ドメイン識別子を対応させて前記端末に表示する表示部（構成情報設定表示部）とを備えることを特徴とする。

【0038】

また、本発明のパケット中継装置は、端末からの指示に基づきドメイン間中継ポリシーテーブルに設定された各送信元VPN識別子（送信元仮想閉域網識別子）および前記各送信元VPN識別子に対応する経路ドメインの一覧を要求する手段と、前記要求に基づいてドメイン間中継ポリシーテーブルから1つ以上の送信元VPN識別子（送信元仮想閉域網識別子）を抽出し、前記各送信元VPN識別子に対応する経路ドメインの一覧を抽出する手段と、抽出された前記各送信元VPN識別子および前記各送信元VPN識別子に対応する経路ドメインの一覧を前記端末に表示する手段を備えることを特徴とする。

【0039】

【発明の実施の形態】

以下、図面を参照しながら本発明の動作原理および好適な実施の態様を説明する。なお、以降、送信元VPN識別子を仮想閉域網識別子と呼び、宛先VPN識別子を宛先仮想閉域網識別子と呼び、送信先VPN識別子を送信先仮想閉域網識別子と呼ぶことがある。また、送信元VPN識別子を送信元VPN、送信先VPN識別子を送信先VPN、経路ドメインをドメインと呼ぶことがある。

【0040】

図4は本発明の中継装置100の動作原理を説明する図である。

【0041】

図中、パケット中継手段51は、入力されたルーティングパケットを経路情報管理手段54に送出し、入力されたパケットをドメイン間中継手段53、ネットワーク間中継手段52及び経路情報管理手段54との連携により得られた情報に基づき中継の対象となるパケットを所望の転送先に送出する。なお、ルーティン

グパケットに含まれるルーティング情報に依存せずに、手作業によりルーティング情報を経路情報管理手段54に設定してもよい。また、ネットワーク間中継手段52は1つ以上の経路ドメインを収容する仮想閉域網（VPN）を対象にしてもよい。

【0042】

前記ネットワーク間中継手段52は、パケット中継手段51から呼び出され、パラメタとしてパケットのヘッダ情報および属性情報を受け取る。次に、該パケットに対応する送信元仮想識閉域網識別子（送信元VPN識別子）に基づき中継可能な仮想識閉域網識別子（送信先VPN識別子）を検索する。

【0043】

そして、ドメイン間中継手段53を呼び出す。そのときに該パケットのヘッダ情報、属性情報、および中継可能な仮想識閉域網識別子（送信先VPN識別子）をパラメタとして渡す。ドメイン間中継手段53は、中継可能な仮想識閉域網が収容される各経路ドメインを特定し、送信先IPアドレスに基づき所望の転送先IPアドレスおよび出力インタフェース情報等、あるいは、中継できない旨の情報を経路情報管理手段54から取得する。それらの情報を最終的にパケット中継手段51に通知する。パケット中継手段51は前記情報に基づき前記パケットを所望の転送先に送出する、あるいは、破棄する。

〈実施の態様1〉

図5は、本発明の第1の実施態様の例を説明する図である。

【0044】

受信インタフェース13は、接続されたネットワーク（例えば、LAN、WAN又はインターネット）からパケットを受信し、それをパケット受信部10に送出する。

【0045】

送信元VPN識別テーブル9は、前記受信インタフェース13を介して受信したパケットの送信元ドメインおよび送信元VPNを識別するためのテーブル（テーブル形式の例は後述する）である。

【0046】

パケット受信部10は、前記ネットワークから前記受信インタフェース13を介して受信したIPパケットのヘッダに設定されている送信先IPアドレスを解析し、このパケットを中継するか、あるいは自局（自ルータ）で受信するかを判定する。

【0047】

また、パケット受信部10は、このパケットを受信した受信インタフェース13の識別子（例えば、ポート番号）をキーとして、送信元VPN識別テーブル9を検索し、このIPパケットがどの経路ドメインおよびどのVPNから受信したかを識別する。なお、送信元VPN識別テーブル9に送信元IPアドレスフィールドを追加すれば、前記検索キーとしてIPパケットヘッダの送信元IPアドレスを用いても同様な結果を得ることができる。

【0048】

パケット受信部10は、自局宛のルーティングパケット（例えば、経路情報を含むBGP-4 [border gateway protocol version 4] パケット等）を受信した場合には、それを経路情報処理部1に送出する。受信したパケットが他の中継装置に中継するパケットである場合にはパケット中継部11に送出する。なお、他の自局宛データパケットについては当業者にとって既知であるので説明を省略する。

【0049】

経路情報処理部1は複数のドメイン内中継テーブル4を有し、通常、ルータが管理する経路ドメインの数に対応して存在する。経路情報処理部1は、パケット受信部10を介して経路情報（ルーティング情報）を含むパケットを受信し、その経路情報の属する経路ドメイン（送信元VPN識別テーブル9から判別される）に対応するドメイン内中継テーブル4（テーブル形式の例は後述する）を更新する。

【0050】

例えば、パケット受信部10は、受信したパケットの受信インタフェース13から送信元VPN識別テーブル9を参照し、送信元の経路ドメインを特定する。そして、特定した経路ドメイン情報と受信した経路情報を経路情報処理部1に送

出する。

【0051】

経路情報処理部1では、パケット受信部10で特定した経路ドメインに基づき対応する1つのドメイン内経路情報管理部2を選択する。選択されたドメイン内経路情報管理部2は前記経路ドメイン情報に対応するドメイン内中継テーブル4を前記経路情報に基づき更新する。なお、中継装置100に設定された経路情報はパケット送信部12を介して他の中継装置（ルータ等）に配布される。

【0052】

各ドメイン内中継テーブル4は、経路ドメインに対応して存在し、経路ドメイン内でのパケットの中継（ルーティング）に必要な経路情報を管理するテーブルである。この各ドメイン内中継テーブル4は手作業により構築してもよい。各ドメイン内中継テーブル4を手作業により構築した場合はドメイン内経路情報管理部1を省略することができる。

【0053】

パケット中継部11は、前記パケット受信部10から受信したパケットを他の中継装置に中継するのに必要な情報を得るためにVPN間中継ポリシ実施部6、VPN定義部5、および各ドメイン内中継テーブル4との連携を行い、出力パケットのヘッダ情報の生成、送信インタフェース14での出力インタフェースを決定し、パケット送信部12へ出力パケットを送出する。

【0054】

更に詳細には、パケット中継部11は、中継するパケットの送信元経路ドメイン、送信元VPN識別子（送信元仮想閉域網識別子）および送信先IPアドレスを呼び出しパラメタにしてVPN間中継ポリシ実施部6を呼び出す。

【0055】

VPN間中継ポリシ実施部6は、送信元VPN識別子（送信元仮想閉域網識別子）と送信先VPN識別子との接続関係（対応関係）を管理するとともに、VPN間中継ポリシテーブル8を前記VPN識別子及び前記送信先IPアドレスを用いて検索し、このパケットを中継できる各VPN識別子の一覧および該各VPN識別子に付帯するIPアドレス情報を取得する。

【 0 0 5 6 】

図示していないが、例えば、前記パケットの送信元のVPN識別子がVPN # 1であり、このVPN # 1に対応する中継可能なVPN識別子として、VPN # 1, VPN # 2, VPN # 4がVPN間中継ポリシーテーブル8に定義されているとすれば、VPN間中継ポリシー実施部6はVPN # 2, VPN # 1, VPN # 4を取得する。

【 0 0 5 7 】

このとき、VPN # 2の優先順位が一番高く、VPN # 4が一番低いものとする。また、VPN # 1に付帯するIPアドレス情報として10.100.123.0/24と定義されていれば、このIPアドレス情報も取得できる。このIPアドレス情報は1つ以上でもよい。また、IPアドレス情報に論理積(AND)、論理和(OR)、論理否定(NOT)、括弧などの論理演算子等、および/または、接続に関する指示(例えば、許可[Permit]、不許可[Deny])等を含めて表現してもよい。

【 0 0 5 8 】

即ち、前記パケットを中継可能なVPN識別子を得られ、その、VPN識別子に付帯する条件として、IPアドレス情報を指定できる。これは、例えば、パケットをVPN # 2に中継可能であっても、付帯条件として指定されたIPアドレス情報が指定された条件に合致しなければそのパケットの中継はできないことになる。例えば、パケットの宛先IPアドレスが10.10.50.50であった場合、前述のIPアドレス情報として「10.10.50.0/24 Deny」と指定されていれば、VPN # 2として中継可能であるが、前記IPアドレス情報によれば該パケットは中継できないことになる。

【 0 0 5 9 】

次に、VPN間中継ポリシー実施部6(図5)はパケット中継部11から受け取った前記送信先IPアドレス、前記送信元経路ドメイン、及びVPN間中継ポリシーテーブル8から取得した1つ以上の各送信先VPN識別子と該各送信先VPN識別子に付帯するIPアドレス情報をパラメタにしてVPN定義部5(図5)を呼び出す。

【0060】

前記VPN定義部5は、送信先VPN識別子と経路ドメイン識別子との接続関係（対応関係）を管理するとともに、パラメタとして受け渡された前記各送信先VPN識別子に対応するドメイン間中継ポリシテーブル7を参照し各ドメイン内中継テーブル4にそれぞれ優先順位を付与する。そして、パラメタとして受け渡された前記送信先IPアドレスを用いて各ドメイン内中継テーブル4を前記優先順位にしたがって検索する。このとき、各送信先VPN識別子に付帯するIPアドレス情報も評価する。この検索結果において、最初に検出された次ホップルータのIPアドレス及び出力インタフェースの情報、あるいは、中継できない（検索の結果、該当する情報を得られなかった）といった情報を得る。なお、ドメイン間中継ポリシテーブル7から中継ポリシとしてフィルタリング情報、アドレス変換のNAT(Network Address Translation)情報なども得ることができる。

【0061】

そして、これらの情報をVPN間中継ポリシ実施部6およびパケット中継部11を介してパケット送信部12に渡す。このとき、パケット中継部11は、中継できないとの情報を受ければ該パケットを破棄する。

【0062】

パケット送信部12はこのパケットを送信すべき次ホップルータのIPアドレス及び出力インタフェースの情報を受け取るとパケット中継部11からパケットのヘッダ情報の付け替え（送信先IPアドレスの付与等）を行い、関連する送信インタフェース情報（出力インタフェース等）を送信インタフェース14に送出する。

【0063】

なお、経路情報処理部1から経路情報を含むパケットを受信した場合は該パケットを指定された送信インタフェース14に送出する。この技術は既知なので詳細は省略する。

【0064】

送信インタフェース14は、前記送信インタフェース情報に基づき出力インタフェースに合わせてパケット送信部12から受信したパケットを送出する。そし

て、この中継装置に接続されたネットワークに送出される。

【 0 0 6 5 】

以上の説明により、VPN間中継ポリシーテーブル8に設定された送信先VPN識別子と送信先VPN識別子との接続可否に関するポリシー、及びドメイン間中継ポリシーテーブル7に設定された送信先VPN識別子と経路ドメインとの接続可否に関するポリシーに基づいてパケットの中継可否を容易に処理することができる。

【 0 0 6 6 】

また、ドメイン間中継ポリシーテーブル7およびVPN間中継ポリシーテーブル8が階層構造に構成されているので、前記ポリシーの設定／変更が容易にできる。

＜実施の態様2＞

図6は本発明の第2の実施態様の例を説明する図である。

【 0 0 6 7 】

第1の実施態様（図5）と第2の実施態様（図6）との本質的な差異は経路情報処理部1に経路フィルタ3を設けることにある。経路フィルタ3は、ドメイン内経路情報管理部2がドメイン内中継テーブル4に設定する経路情報を制限（フィルタリング）するためのフィルタである。

【 0 0 6 8 】

例えば、図6に示す例では、経路フィルタ3を1つの経路ドメインに対してのみ設けているが、経路情報処理部1において複数または全てのドメイン内経路情報管理部2に対応して設けてもよい。

【 0 0 6 9 】

この経路フィルタ3はドメイン内経路情報管理部2から対応するドメイン内中継テーブル4に経路情報を設定するが、その際、経路フィルタ3が介在している場合は、この経路フィルタで指定された条件の経路情報のみを通過させる。

【 0 0 7 0 】

経路フィルタ3にIPアドレスとして、例えば、192.169.30.0／24が指定された場合、全32ビット中、先頭ビットから24ビット（IPアドレスの最後に「／24」を付加して記述する）と一致するIPアドレス（192.169.30.*）[*は0～255の任意値を示す]に関する経路情報の

設定を明示的に禁止する、あるいは、前記 IP アドレスのみの設定を許可することにより、この経路フィルタで許可された経路情報のみをドメイン内経路情報管理部 2 に設定することができる。

【 0 0 7 1 】

このようにして、1つの経路ドメインに対して経路フィルタ 3 により上位 n ビット（前述の例では先頭 24 ビット）を用いて IP アドレスを 1 つ以上にグループ化し、そのグループの論理和などの処理を行うことにより、同一ドメイン内のポリシーの設定において、更に細かな IP アドレスのグルーピングによるポリシーの設定が可能になる。

＜実施の態様 3＞

第 3 の実施態様は第 2 の実施態様の変形例の 1 つであり、図 7 は、本発明の第 3 の実施態様の例を説明する図である。

【 0 0 7 2 】

第 3 の実施態様（図 7）と第 2 の実施態様（図 6）との本質的な差異は、経路フィルタ 3 A により分割された複数のドメイン内中継テーブル 4 A を対応させて経路情報を設定できる点にある。

【 0 0 7 3 】

すなわち、ある IP アドレスグループを有する 1 つの経路ドメインを 2 つ以上に分割して運用する場合、経路情報処理部 1 の対応するドメイン内経路情報管理部 2 に経路フィルタ 3 A を設けることにより少ない作業量で、分割された経路ドメインに対応する複数のドメイン内中継テーブル 4 を効率的に構築することができる。

【 0 0 7 4 】

例えば、一つの経路ドメインを 2 つの経路ドメインに分割して新たな運用を行う場合、分割された各経路ドメインに対応する 2 つの IP アドレスグループがあるとする。図示していない第 1 グループの IP アドレスは、192. 168. 10. 0 / 24 であり、第 2 グループは 192. 168. 20. 0 / 24 とする。

【 0 0 7 5 】

このような場合、経路フィルタ 3 A により第 1 グループの経路情報をドメイン

内中継テーブル 4 A に設定し、第 2 グループの経路情報を対応するドメイン内中継テーブル 4 B に設定することができる。

【 0 0 7 6 】

このように、1 つの経路ドメインを 2 つ以上の経路ドメインに分割した場合には、上述のように I P アドレスグループ単位に対応する複数のドメイン内中継テーブル 4 に経路情報の設定を制御することができる。

＜実施の態様 4＞

第 4 の実施態様は第 1 の実施態様の変形であり、図 8 に本発明の第 4 の実施態様の例を説明する図を示す。

【 0 0 7 7 】

第 4 の実施態様（図 8）と第 1 の実施態様（図 3）との本質的な差異は、V P N 定義部 5 と構成情報設定表示部 1 5 との連携、および V P N 間中継ポリシー実施部 6 と構成情報設定表示部 1 5 との連携にある。

【 0 0 7 8 】

すなわち、構成情報設定表示部 1 5 に接続された端末 1 6（例えば、ワークステーションなど）からの指令に基づきドメイン間中継ポリシーテーブル 7 及び V P N 間中継ポリシーテーブル 8 に設定された情報を端末 1 6 から指定された条件に基づいて表示／更新（変更、追加、削除）することにある。

【 0 0 7 9 】

この端末 1 6 は回線（W A N、L A N、インターネットあるいは電話回線等）を介して接続されたりリモート端末（例えば、P C 等）であってもよい。

【 0 0 8 0 】

詳細には、構成情報設定表示部 1 5 は、構成情報設定表示部 1 5 に接続された端末 1 6 からのコマンド等の指令により、V P N 間中継ポリシーテーブル 8 に定義された各送信元 V P N 識別子（送信元仮想閉域網識別子）および該各送信元 V P N 識別子に対応する送信先 V P N 識別子（送信先仮想閉域網識別子）の一覧の要求を V P N 間中継ポリシー実施部 6 に依頼する。

【 0 0 8 1 】

V P N 間中継ポリシー実施部 6 はその要求に基づいて、V P N 間中継ポリシテ

ブル 8 を参照し、設定されているすべての V P N 識別子を検索し、各送信元 V P N 識別子（送信元仮想閉域網識別子）に対応する送信先 V P N 識別子の一覧を構成情報設定表示部 1 5 に渡す。

【 0 0 8 2 】

そして、端末 1 6 に図 9 に示す送信元 V P N の一覧を表示するメニュー（ウインドウ）の例を表示する。

【 0 0 8 3 】

端末 1 6 の画面（ウインドウ）から特定の送信先 V P N 識別子が入力された場合、例えば、図 9 に図示された送信元 V P N として「V P N 2」をクリックした場合には「送信元 V P N 2」が構成情報設定表示部 1 5 に入力される。

【 0 0 8 4 】

構成情報設定表示部 1 5 は、送信元 V P N 2 に対応する宛先 V P N（送信先 V P N）に関する情報の取得を V P N 間中継ポリシー実施部 6 に依頼する。

【 0 0 8 5 】

V P N 間中継ポリシー実施部 6 は、指定された送信元 V P N 識別子（送信元仮想閉域網識別子）である「V P N 2」に対応する宛先 V P N 識別子（送信先仮想閉域網識別子）を求めるために V P N 間中継ポリシーテーブル 8 を検索し、その結果を構成情報設定表示部 1 5 に通知する。

【 0 0 8 6 】

構成情報設定表示部 1 5 は通知された宛先 V P N 識別子の数が 1 つ以上であれば、その各宛先 V P N 識別子に対応する送信先経路ドメインの検索を V P N 定義部 5 に依頼する。V P N 定義部 5 は前記各宛先 V P N 識別子に基づき V P N 間中継ポリシーテーブル 7 を検索し、対応する各経路ドメイン識別子を取得する。

【 0 0 8 7 】

その取得結果を V P N 定義部 5 に通知する。V P N 定義部 5 は構成情報設定表示部 1 5 に、各宛先 V P N 識別子および各経路ドメイン識別子を対応づけて通知する。構成情報設定表示部 1 5 は、前記送信元 V P N 識別子とそれに対応する各宛先 V P N 識別子、及び該各宛先 V P N 識別子に対応する各経路ドメイン識別子を G U I（G r a p h i c a l U s e r I n t e r f a c e）として端末 1

6の画面上に表示する。前記画面のウィンドウに表示する例を図10に示す。

【0088】

なお、前述の説明では、端末画面上への表示を中心に説明したが、表示した情報（送信元VPN識別子、宛先VPN識別子（送信先VPN識別子）、送信先経路ドメイン識別子）に対する追加、変更、削除の方法について説明する。

【0089】

例えば、送信元VPN識別子（送信元仮想閉域網識別子）を追加登録する例を説明する。

【0090】

端末16の画面上に図9に示すメニュー（ウィンドウ）が表示されている状態において、ファンクションキー（PF1～PF12）のうち、例えば、PF5を押下すると、「VPN3」と表示されている下に、新たな送信元VPN識別子を追加登録するための入力を指示が、例えば、図11のように表示される。

【0091】

その指示に従って追加登録すべき送信元VPN識別子が入力された場合、構成情報設定表示部15はこの入力に基づきVPN間中継ポリシ実施部6に前記送信元VPN識別子の追加処理を依頼する。そして、VPN間中継ポリシ実施部6はVPN間中継ポリシテーブル8に前記送信元VPN識別子の追加登録を行う。そして、端末16は次の指示入力待ち状態となる。

【0092】

送信元VPN識別子の削除は、例えば、図9に表示されている状態において、PF6キーを押下することにより、例えば、図12に示すメニューが表示される。

【0093】

そして、削除すべき送信元VPN識別子が入力された場合には、構成情報設定表示部15はこの指示に基づきVPN間中継ポリシ実施部6に指定された送信元VPN識別子の削除を依頼する。そして、VPN間中継ポリシ実施部6はVPN間中継ポリシテーブル8に前記送信元VPN識別子の削除を行う。そして、端末16は次の指示入力待ち状態となる。

【 0 0 9 4 】

送信元VPN識別子の変更は、例えば、図9に表示されている状態において、例えば、カーソルを変更したい送信元VPN識別子の上に置き、そしてPF7キーを押下することにより、例えば、図13に示すメニュー（ウインドウ）が表示される。

【 0 0 9 5 】

また、送信元VPN識別子の変更指示が入力された場合には、構成情報設定表示部15はこの指示に基づきVPN間中継ポリシー実施部6に、変更前の現送信元VPN識別子と変更後の新送信元VPN識別子をパラメタにして変更を依頼する。

【 0 0 9 6 】

構成情報設定表示部15はこのパラメタに基づきVPN間中継ポリシー実施部6に指定された現送信元VPN識別子を新送信元VPN識別子に変更する処理を依頼する。そして、VPN間中継ポリシー実施部6はVPN間中継ポリシーテーブル8の現送信元VPN識別子の変更を行う。そして、端末16は次の指示入力待ち状態となる。

【 0 0 9 7 】

構成情報設定表示部15は、端末16から宛先VPN識別子（図10の右側）の追加／削除／変更の入力を受信した場合には、構成情報設定表示部15はこの指示に基づきVPN間中継ポリシー実施部6に指定された宛先VPN識別子の一覧の更新（追加、削除、または変更）処理を依頼する。

【 0 0 9 8 】

図示していないが、これらの宛先VPN識別子の変更処理の依頼も前述と同様にPFキー8（追加）、変更の対象となる宛先VPN識別子の上にカーソルを置いてPFキー9（削除）を押下、変更の対象となる宛先VPN識別子の上にカーソルを置いてPFキー10（変更）を使用することにより、同様に、構成情報設定表示部15はVPN間中継ポリシー実施部6に前記宛先VPN識別子の更新（追加、削除または変更）を依頼する。

【 0 0 9 9 】

VPN間中継ポリシー実施部6は前記依頼に基づいてVPN間中継ポリシーテーブル8の更新（追加、削除、または変更）を行う。

【0100】

図14は、図9に示すメニュー（ウインドウ）において送信元VPN3をクリックした場合に表示される情報の例であり、主たる情報の構造は図10と同じである。しかしながら、図14には属性情報1～4が表示されているが、図10には表示されていない点で異なる。なお、属性情報1～4は、初期画面に表示されていない。

【0101】

これらの属性情報は、送信元VPN識別子または宛先VPN識別子にカーソル移動する、あるいは、それをクリックするとそのVPN識別子に関する属性情報が端末16に表示される。

【0102】

より詳細には、例えば、端末16の画面上に表示された送信元VPN識別子（VPN3）、宛先VPN識別子（VPN3、VPN1）、ドメイン名（ドメイン4、ドメイン1、及びドメイン2）の上にカーソルを移動させると、構成情報設定表示部15にカーソルがその表示対象に移動したことが通知される。

【0103】

構成情報設定表示部15は通知された情報に基づきVPN識別子を特定する。例えば、特定された対象が送信元VPN3であるとすれば、該VPN3に関する属性情報1を前述したようにVPN間中継ポリシーテーブル8を検索し、取得した属性情報1を画面上に表示する。

【0104】

同様に、属性情報2の表示では、構成情報設定表示部15は通知された指示にしたがって、宛先VPN2をパラメタとしてVPN定義部5を呼び出し、対応する属性情報2の抽出を依頼する。そして、VPN定義部5は属性情報2を抽出し構成情報設定表示部15に通知する。

【0105】

構成情報設定表示部15は、通知された宛先VPN2の属性情報2を端末16

に表示する。端末装置 16 における表示の例を図 14 に示す。

【0106】

更に、構成情報設定表示部 15 が端末 16 に属性情報 2 を表示中に、例えば、PF11 キーを押下すると表示名の属性情報 2 を更新することができる状態になる。

【0107】

表示された属性情報 2 の各項目の変更は、上書きすることにより変更することができる。例えば、宛先アクセス優先度 1 の右側に「ドメイン 4」と値が表示されているが、これを、「ドメイン 3」と設定し直す（タイプインする）と「ドメイン 4」を「ドメイン 3」に変更することができる。

【0108】

また、削除キーを使って、表示された「ドメイン 4」を削除する、あるいは、空白により上書きすると、「ドメイン 4」は削除される。

【0109】

また、PF12 キーを押下すると、「ドメイン 4」の下に新たな入力フィールドが現れ、追加登録すべき送信先経路ドメインの入力が可能になる。この入力フィールドに、例えば、「ドメイン 5」を入力すると、既に設定されている「ドメイン 4」の他に「ドメイン 5」を追加登録することができる。

【0110】

同様に、Owner、アクセスルール、フィルタ条件の各フィールド値も変更することができる。

【0111】

また、端末 16 の画面（ウインドウ）から送信先経路ドメインの編集（追加、削除、または変更）を想定する。例えば、図 11 に図示された「ドメイン 4」を端末 16 のウインドウ上に表示された宛先 VPN 3 配下の「ドメイン 4」をクリックした場合には「宛先 VPN 3 のドメイン 4」が構成情報設定表示部 15 に入力される。

【0112】

構成情報設定表示部 15 は、「宛先 VPN 3 のドメイン 4」をパラメタとして

、VPN定義部5に属性情報3の取得を依頼する。VPN定義部5はドメイン間中継ポリシーテーブル7から送信先VPN識別子である宛先VPN3およびドメイン4の属性情報3を取得し、構成情報設定表示部15に通知する。

【0113】

構成情報設定表示部15は、通知された属性情報3を端末16に表示する。表示の例を図11の右上に示す。

【0114】

図15は送信元VPN識別子に関する情報（送信元VPN識別子、送信先VPN識別子、経路ドメイン識別子）を既に説明した同様な手順により取得できることは明らかである。よって、ここでは、図15を使ってその情報の表示方法を説明する。

【0115】

図中、3つウィンドウが表示されており、ウィンドウ1がルートウィンドウであり、図9に示す画面表示内容と同じ表示内容である。ウィンドウ2はウィンドウ1内に表示されている送信元VPN識別子の内表示対象（この図ではVPN3）を左クリックするとウィンドウ2が新たに表示される。右クリックすると属性情報1が表示される。

【0116】

ウィンドウズ2が表示された状態で表示対象（この図では上段の宛先VPN3）を右クリックすると属性情報2が表示される。一方、左クリックするとウィンドウ3が新たに表示され、そのウィンドウ内に前記宛先VPN3に対応する経路ドメイン4が表示される。

【0117】

ウィンドウ3の経路ドメイン4を右クリックすると属性情報3が表示される。

【0118】

以上のように階層的に、例えば、ウィンドウ1～3のように、送信元VPN識別子、宛先VPN識別子（送信先VPN識別子）、宛先（送信先）経路ドメイン識別子の関係を階層的に端末16に表示することにより、送信元VPNに関連する設定情報を容易に確認することができる。

【 0 1 1 9 】

特に、GUIを介して前記階層化された送信元VPN識別子に対応する情報を視覚的に整理された情報として端末画面上に表示することができる。なお、情報が多い場合には1つのウィンドウ（論理画面）を複数の物理画面（端末画面）に分割して個々を1画面として表示する、あるいは、スクロール機能により連続的移動表示することにより、全体情報を容易に把握することができる。

【 0 1 2 0 】

以上のように、ドメイン間中継ポリシーテーブル7およびVPN間中継ポリシーテーブル8の情報を端末16に表示／更新することにより設定情報を容易に確認することができる。更に、確認した設定情報を変更したい場合には、その値を確認しながら変更、追加、削除を容易に行うことができる。

＜実施の態様5＞

図16は本発明の第1の実施態様を適用したルータをプロバイダが提供するネットワークに採用した例を説明する図である。なお、この実施例では、プロバイダが提供するVPNサービスと同等なVPNサービスをキャリアが提供する場合、該キャリアは該プロバイダに含まれるものとする。

【 0 1 2 1 】

図17は図16に示すネットワークのドメイン構成を説明する図である。

【 0 1 2 2 】

図18は図16に示すルータ1における受信インタフェースと送信元ドメイン及び送信元VPNとの対応を管理する送信元VPN識別テーブル9の例を説明する図である。

【 0 1 2 3 】

図19はVPN間の中継ポリシーを設定するテーブルの形式の例を説明する図である。

【 0 1 2 4 】

図20はドメイン間中継ポリシーを設定するテーブルの形式及び設定値の例を説明する図である。図21、図22および図23は経路ドメイン間における中継テーブルの形式及び設定値の例を説明する図である。

【 0 1 2 5 】

図 1 6 乃至図 2 3 を参照しながら本発明を適用したルータの動作例を説明する。

【 0 1 2 6 】

図 1 6 に示すプロバイダ網が V P N サービスを提供するネットワークには、4 つの経路ドメイン（ドメイン # 1 ～ドメイン # 4）が存在し、3 つルータ（ルータ 1 ～ルータ 3）が存在している。

【 0 1 2 7 】

このうちドメイン # 1, # 2, # 4 を管理しているルータ 1（I P アドレスは 192.168.254.1）に着目して、本発明を適用したルータ 1 の動作例を説明する。なお、ルータ 2 またはルータ 3 は本発明を適用してなくてもよいが、適用してもよい。まず、V P N サービスを提供するルータ 1 の一般的な動作を説明し、V P N 間および経路ドメイン間の接続性可否の処理説明は後述する。

【 0 1 2 8 】

ルータ 1 は、収容する各経路ドメインに対応する各ドメイン内中継テーブルを備え、それぞれ独立に管理している。経路ドメイン # 1, # 2, # 4 に対応させて構築した各ドメイン内中継テーブル 4 の形式の例を図 2 1 ～図 2 3 に示す。

【 0 1 2 9 】

ルータ 1 は、受信インタフェース I F 0 ～ I F 2（図 1 6）からそれぞれパケットを受信するとパケット毎に送信元 V P N 識別テーブル 9（図 1 6）を参照し、その受信パケットが属する経路ドメインを調べ、その経路ドメインに対応するドメイン内中継テーブル 4（図 2 1 ～図 2 3）を参照し、次に中継する次ホップルータの I P アドレスおよび出力インタフェースを求める。そして、そのパケットのヘッダを作成し、出力インタフェース I F 1 0 ～ I F 1 2（図 1 6）の選択されたいずれかから次ホップルータに送出する。

【 0 1 3 0 】

例えば、ルータ 1 が、受信インタフェース I F 0（図 1 6）から送信先 I P アドレスが 192.168.100.10（経路ドメイン # 2, V P N # 1）であるデータパケットを受信すると、まず、ルータ 1 は送信元 V P N 識別テーブル 9（図 1 8）を参照し

、受信インタフェースIF0（図16）から受信したパケットがドメイン#2に属し、送信元VPN識別子がVPN#1であることを特定する。

【0131】

次に、VPN間中継ポリシーテーブル8を検索して得られた、送信元VPN識別子から中継可能なVPNであるVPN#1を構成する経路ドメインをドメイン間中継ポリシーテーブル7から検索し、VPN#1に対してはドメイン#1およびドメイン#2を取得する。

【0132】

次に、VPN#1と経路ドメインとの接続性を検索する。すなわち、VPN#1を検索キーとしてドメイン間中継ポリシーテーブル7（図20）を検索する。その結果、重複情報を削除し、ドメイン#1およびドメイン#2を得る。

【0133】

次に、送信先IPアドレス（192.168.100.10）をキーとして、ドメイン#1およびドメイン#2に対応するドメイン内中継テーブル4（図21，図22）を優先順序に従って、図21、次に図22を検索する。この検索は、複数のプロセッサを使用して並列処理を行ってもよい。この検索の結果、最初に検出された次ホップルータアドレスを採用する。

【0134】

経路ドメイン2のドメイン内中継テーブル4（図22）から次ホップルータのIPアドレスとして192.168.254.3および出力インタフェースとしてIF10を得る。すなわち、このパケットは中継可能である。

【0135】

そして、次ホップルータとしてルータ3（192.168.254.3）に前記パケットを送出する。

【0136】

また、本実施の態様では、例えば、プロバイダは図16に示した経路ドメイン間での接続の許可／不許可を図17に示すように接続性を定義しているものとする。経路ドメイン#1（10.25.0.0）と経路ドメイン#2（192.168.0.0）はVPN#1として相互に接続性を持ち、プロバイダ網を介してエクストラネットを構成し

ている。また、経路ドメイン # 2 (192.168.0.0) と経路ドメイン # 3 (10.30.0.0) は VPN # 2 として相互に接続性を持ち、プロバイダ網を介してエクストラネットを構成している。

【 0 1 3 7 】

経路ドメイン # 1 (10.25.0.0) と経路ドメイン # 3 (10.30.0.0) は相互に通信できる接続性は定義されていない。また、経路ドメイン # 4 (192.172.0.0) は単一の経路ドメインから成り、イントラネットとして VPN # 3 を構成している。

【 0 1 3 8 】

上述のネットワークにおいて、例えば、VPN # 1 (経路ドメイン # 1 と # 2 とのエクストラネット接続) と VPN # 3 (経路ドメイン # 4 でのイントラネット接続) との VPN 間通信ポリシー (フィルタ条件、アドレス変換処理等) を定義するものとする。アドレス変換処理とは、イントラネット内のみで使用されるローカル IP アドレスを独自に割り当てて運用し、イントラネットとインターネット間でパケットが送信/受信されるときにイントラネット内のローカル IP アドレスとグローバル IP アドレスとを相互に変換する処理を示す。このアドレス変換については、IETF (Internet Engineering Task Force) が標準化した RFC 1631 等で既に規定されているので、詳細はこれを参照されたい。

【 0 1 3 9 】

次に、図 19 はルータ 1 において VPN # 1 ~ VPN # 3 との間における中継ポリシーの設定例を説明する図である。これによると、ルータ 1 は、VPN # 1 からパケットを受信した場合は、VPN # 1 は無条件でパケットを中継可能であるが、他の VPN (例えば VPN # 3 など) パケットを中継することはできない。

【 0 1 4 0 】

一方、VPN # 3 からパケットを受信したルータ 1 は、VPN # 3 には無条件でパケット中継することが可能である。しかしながら、送信先が VPN # 1 である場合は、送信先アドレスとして 192.172.10.0/24 を有するパケットを排除するフィルタ処理 (図 6 に示す経路フィルタ 3 により処理される) が示されている。

【 0 1 4 1 】

まず、VPN # 1 及び VPN # 3 を構成するドメイン間の中継ポリシーを図 20

に示すように設定されるものとする。この設定によると、VPN # 1 は、ドメイン # 1 とドメイン # 2 との接続性を持ち、どちらのドメインへも無条件で中継可能(permit)であることを示している。このとき、ドメイン # 1 の方をドメイン # 2 より優先してドメイン内中継テーブルを参照することを示している。

【 0 1 4 2 】

また、VPN # 3 については、ドメイン # 4 (ルータ 1 の IF2 とルータ 2 の IF2 との接続) のみから構成され、ドメイン # 4 内のパケット転送は無条件の中継が許可されていることを示している。

【 0 1 4 3 】

以上、上述したように第 1 の実施態様を適用したルータをプロバイダ網に適用することにより、プロバイダは VPN サービスをエンドユーザに提供することができる。

(付記 1) 入力されたパケットに対応する送信元仮想閉域網識別子に基づき、該パケットの中継が許されている 1 つ以上の仮想閉域網を選択する手段と、

前記 1 つ以上の仮想閉域網に対応する 1 つ以上の経路ドメインを選択する手段と、

前記パケットの送信先アドレスと前記 1 つ以上の経路ドメインの各経路ドメイン情報とを照合し、前記パケットを次のパケット中継装置に送出するための送出先アドレス(次ポップルータアドレス)を選択する手段と、

前記送出先アドレスに前記パケットを送出する手段を有することを特徴とするパケット中継装置。

(付記 2) 付記 1 記載において、

前記パケットの送信元仮想閉域網および前記 1 つ以上の仮想閉域網の少なくとも 1 つは仮想私設網であることを特徴とするパケット中継装置。

(付記 3) 付記 1 記載において、

前記経路情報管理手段は経路情報をフィルタする経路フィルタを具備し、

前記経路フィルタにより選択された経路情報をドメイン内中継テーブルに設定することを特徴とするパケット中継装置。

(付記 4) 付記 1 記載において、

前記経路情報管理手段は経路情報（destination）をフィルタする経路フィルタを具備し、

ドメイン間パケット中継手段が管理するドメイン内中継テーブルに経路情報を設定するときに、前記経路情報を複数のドメイン内中継テーブルに分割して書き込むことを特徴とするパケット中継装置。

（付記 5） 入力されたパケットの送信元仮想閉域網識別子に基づき、該パケットを中継できる 1 つ以上の仮想閉域網を選択するステップと、

前記 1 つ以上の仮想閉域網に対応する 1 つ以上の経路ドメインを選択するステップと、

前記パケットの送信先アドレス（次ポップルータアドレス）と前記 1 つ以上の経路ドメインの各経路情報（destination）とを照合し、前記パケットの送出先アドレスを選択するステップと、

前記送出先アドレスに前記パケットを送出するステップを有することを特徴とするパケット中継方法。

（付記 6） 複数の送信元仮想閉域網識別子と該各送信元仮想閉域網識別子に対応する 1 つ以上の宛先仮想閉域網識別子を管理するポリシー管理部（VPN 間中継ポリシー実施部）と、

前記ポリシー管理部から 1 つ以上の送信元仮想閉域網識別子と該 1 つ以上の各送信元仮想閉域網識別子に対応する 1 つ以上の宛先仮想閉域網識別子を該 1 つ以上の各送信元仮想閉域網識別子に対応させて端末に表示する表示部（構成情報設定表示部）と

を備えることを特徴とするパケット中継装置。

（付記 7） 付記 6 記載において、

前記ポリシー管理部は、前記表示部が前記端末から受け取る 1 つの送信元仮想閉域網識別子に対応する 1 つ以上の宛先仮想閉域網識別子を前記表示部に送出し、

前記表示部は、前記 1 つの送信元仮想閉域網識別子と前記 1 つ以上の宛先仮想閉域網識別子に対応させて前記端末に表示することを特徴とするパケット中継装置。

（付記 8） 前記各宛先仮想閉域網識別子と該各宛先仮想閉域網識別子に対応す

る 1 つ以上の経路ドメイン識別子を管理する仮想閉域網管理部（VPN 定義部）を備え、

前記仮想閉域網管理部は前記端末から入力される 1 つの宛先仮想閉域網識別子と該 1 つの宛先仮想閉域網識別子に対応する 1 つ以上の経路ドメイン識別子に対応させて前記端末に表示する表示部（構成情報設定表示部）と

を備えることを特徴とするパケット中継装置。

（付記 9） 付記 6 記載において、

前記表示部は、前記端末から追加登録すべき送信元仮想閉域網識別子を受け取って前記ポリシー管理部（VPN 間中継ポリシー実施部）に追加の登録を依頼し、

前記ポリシー管理部は送信元仮想閉域網識別子を VPN 間中継ポリシーテーブルに登録することを特徴とするパケット中継装置。

（付記 10） 付記 6 記載において、

前記表示部は、前記端末から受け取った削除すべき送信元仮想閉域網識別子の削除を前記ポリシー管理部に依頼し、

前記ポリシー管理部は該送信元仮想閉域網識別子を VPN 間中継ポリシーテーブルから削除することを特徴とするパケット中継装置。

（付記 11） 付記 6 記載において、

前記表示部は、前記端末から受け取った名称を変更すべき現送信元仮想閉域網識別子と新送信元仮想閉域網識別子を前記ポリシー管理部に名称の変更を依頼し、

前記ポリシー管理部は、VPN 間中継ポリシーテーブルに存在する前記現送信元仮想閉域網識別子の名称を新送信元仮想閉域網識別子に変更することを特徴とするパケット中継装置。

（付記 12） 端末からの指示に基づきドメイン間中継ポリシーテーブルに設定された各送信元仮想閉域網識別子および前記各送信元仮想閉域網識別子に対応する経路ドメインの一覧を要求する手段と、

前記要求に基づいてドメイン間中継ポリシーテーブルから 1 つ以上の送信元仮想閉域網識別子を抽出し、前記各送信元仮想閉域網識別子に対応する経路ドメインの一覧を抽出する手段と、

抽出された前記各送信元仮想閉域網識別子および前記各送信元仮想閉域網識別

子に対応する経路ドメインの一覧を前記端末に表示する手段を備えることを特徴とするパケット中継装置。

(付記 1 3) 端末からの指示により、ドメイン間中継ポリシーテーブルに設定された各送信先仮想閉域網識別子および各送信先仮想閉域網識別子に対応する 1 つ以上の経路ドメイン識別子の一覧を要求する手段と、

前記要求に基づいて、ドメイン間中継ポリシーテーブルからドメイン識別子を検索し、各送信先仮想閉域網識別子に対応するドメイン識別子の一覧を抽出する手段と、

前記端末に各送信先仮想閉域網識別子に対応するドメイン識別子の一覧を表示するとともに送信先仮想閉域網識別子の追加登録の指示を端末から受け取る手段と、

前記ドメイン間中継ポリシーテーブルに前記端末から受け取った送信先仮想閉域網識別子の追加登録を行う手段を備えることを特徴とするパケット中継装置。

(付記 1 4) 端末からの指示により、ドメイン間中継ポリシーテーブルに設定された各送信先仮想閉域網識別子および各送信先仮想閉域網識別子に対応するドメイン識別子の一覧を要求する手段と、

前記要求に基づいて、ドメイン間中継ポリシーテーブルを参照して設定されている送信先仮想閉域網識別子を検索し、各送信先仮想閉域網識別子に対応するドメイン識別子の一覧を作成する手段と、

各送信先仮想閉域網識別子に対応するドメイン識別子一覧を端末に表示するとともに該ドメイン識別子の一覧について、送信先仮想閉域網識別子の追加またはドメイン識別子一覧を削除する指示を受け取る手段と、

指示された該追加または該削除に基づき前記ドメイン間中継ポリシーテーブルの更新を行う手段と

を備えることを特徴とするパケット中継装置。

【 0 1 4 4 】

【発明の効果】

本発明によれば、複数の経路ドメイン間相互の中継ポリシーを定義する際に、複数の経路ドメインをいくつかのグループに分け、グループ間の中継ポリシーとして

定義することを可能にする。このことにより定義する中継ポリシーの数が減るため、設定／変更を容易に行える。

【 0 1 4 5 】

また、中継に必要な経路情報を格納する中継テーブルのサイズを小さくすることができる。

【図面の簡単な説明】

【図 1】

シングルドメイン／マルチドメイン，イントラネット／エクストラネットの組み合わせによるネットワーク構成の例を説明する図である。

【図 2】

マルチドメイン構成のリクストラネットVPNを収容するルータの中継テーブルの構成例を説明する図である。

【図 3】

マルチドメイン構成のエクストラネットVPNを収容するルータの中継テーブルの構成例を説明する図である。

【図 4】

本発明の動作原理を説明する図である。

【図 5】

本発明の第 1 の実施態様の例を説明する図である。

【図 6】

本発明の第 2 の実施態様の例を説明する図である。

【図 7】

本発明の第 3 の実施態様の例を説明する図である。

【図 8】

本発明の第 4 の実施態様の例を説明する図である。

【図 9】

本発明の第 4 の実施態様の例における送信元VPNの表示の例を説明する図。

【図 1 0】

本発明の第 4 の実施態様の例における送信元VPNと宛先VPN、宛先ドメイン

ンとの対応関係の表示の例を説明する図。

【図 1 1】

本発明の第 4 の実施態様の例における送信元 V P N を追加するメニューの表示の例を説明する図。

【図 1 2】

本発明の第 4 の実施態様の例における削除すべき送信元 V P N を入力するメニューの表示の例を説明する図。

【図 1 3】

本発明の第 4 の実施態様の例における内証を変更すべき送信元 V P N を入力するメニューの表示の例を説明する図。

【図 1 4】

本発明の第 4 の実施態様の例におけるツリー構造による V P N 管理情報の表示の例を説明する図。

【図 1 5】

本発明の第 4 の実施態様の例におけるマルチウインドウによる V P N 管理情報の表示の例を説明する図。

【図 1 6】

本発明の第 1 の実施態様を適用したルータをプロバイダが提供するネットワークに採用した例を説明する図である

【図 1 7】

図 1 6 に示すネットワークのドメイン構成を説明する図である。

【図 1 8】

図 1 6 に示すルータ 1 における受信インタフェースと送信元ドメイン及び送信元 V P N 識別子との対応を管理する送信元 V P N 識別テーブルの例を説明する図である。

【図 1 9】

V P N 間の中継ポリシを設定するテーブルの形式の例を説明する図である。

【図 2 0】

ドメイン間中継ポリシを設定するテーブルの形式及び設定値の例を説明する図

である。

【図 2 1】

経路ドメイン間における中継テーブルの形式及び設定値の例を説明する図である。

【図 2 2】

経路ドメイン間における中継テーブルの形式及び設定値の例を説明する図である。

【図 2 3】

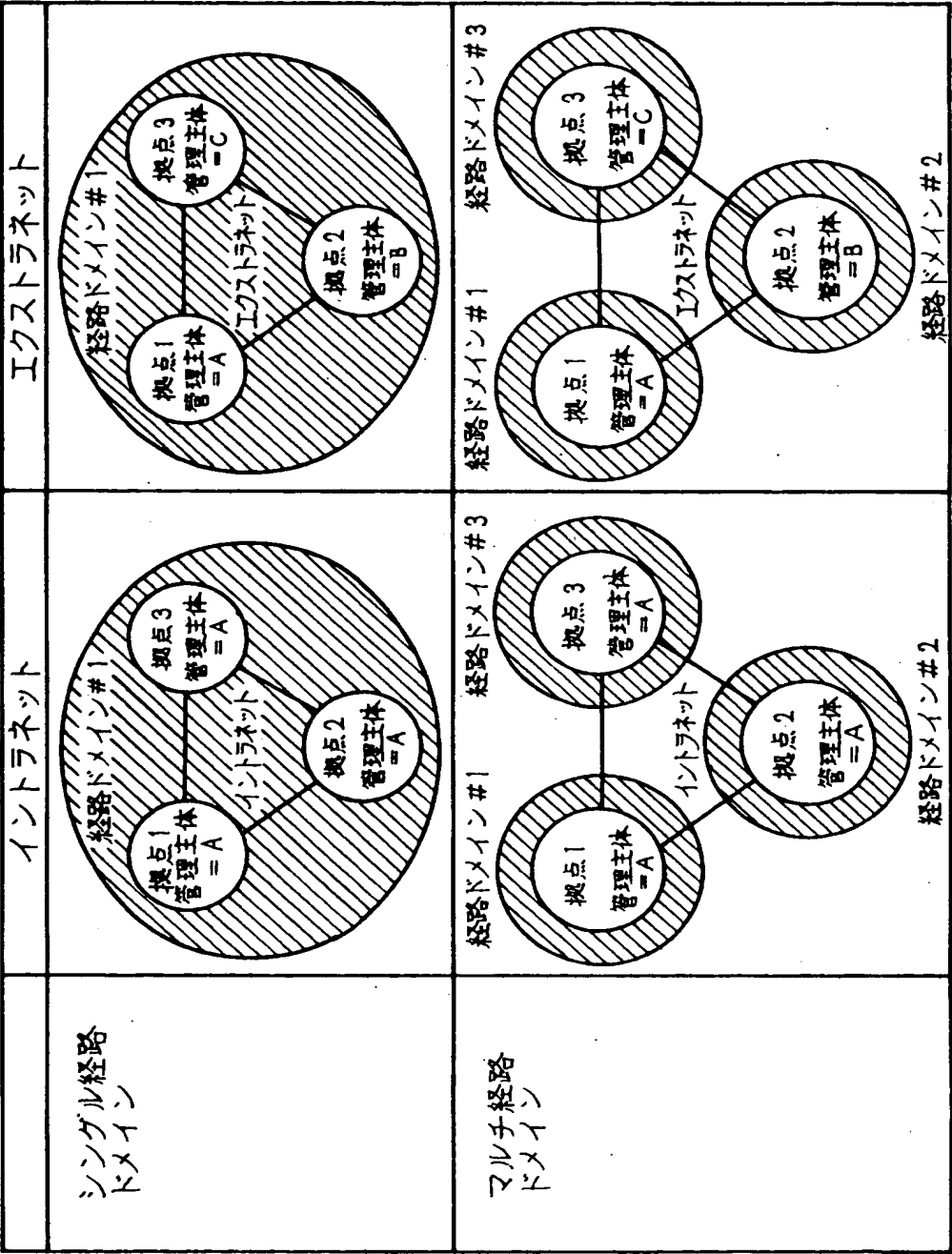
経路ドメイン間における中継テーブルの形式及び設定値の例を説明する図である。

【符号の説明】

- 1 経路情報処理部
- 2 ドメイン内経路情報管理部
- 3 経路フィルタ
- 4 ドメイン内中継テーブル
- 5 VPN定義部
- 6 VPN間中継ポリシー実施部
- 7 ドメイン間中継ポリシーテーブル
- 8 VPN間中継ポリシーテーブル
- 9 送信元VPN識別テーブル
- 10 パケット受信部
- 11 パケット中継部
- 12 パケット送信部
- 14 送信インタフェース
- 51 パケット中継手段
- 52 ネットワーク間中継手段
- 53 ドメイン間中継手段
- 54 経路情報管理手段
- 100 中継装置

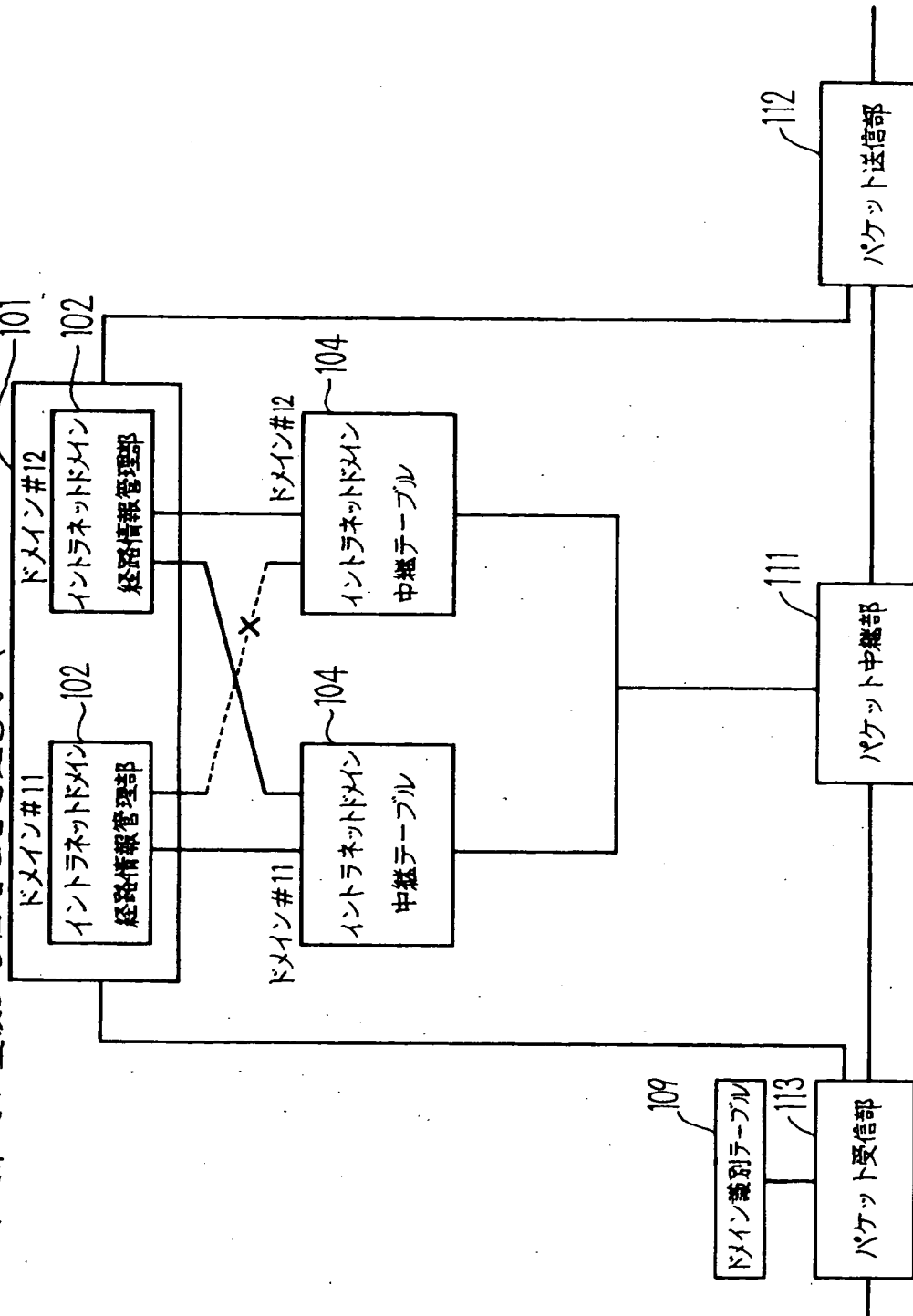
【書類名】 図面
【図 1】

VPNの運用形態

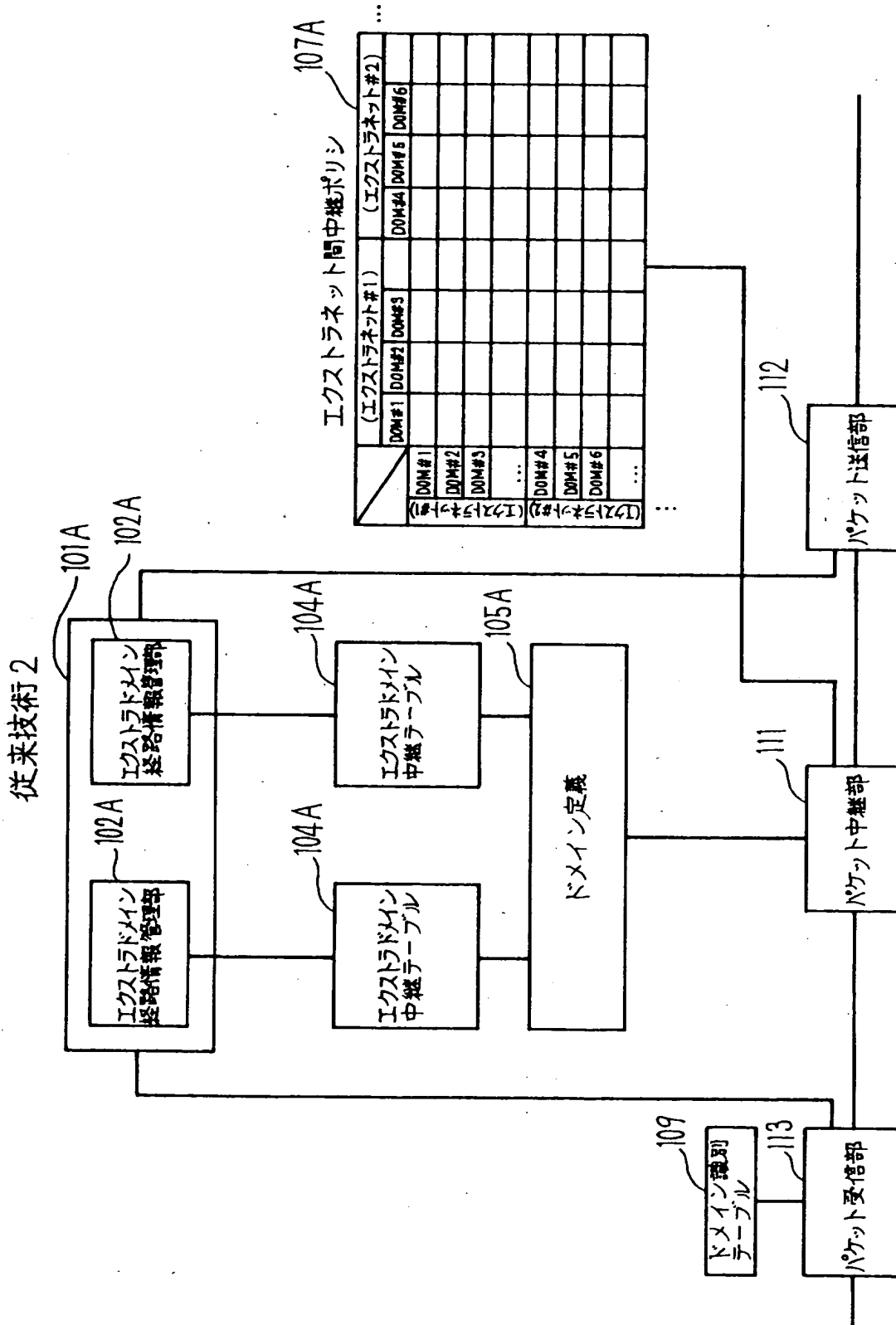


【図 2】

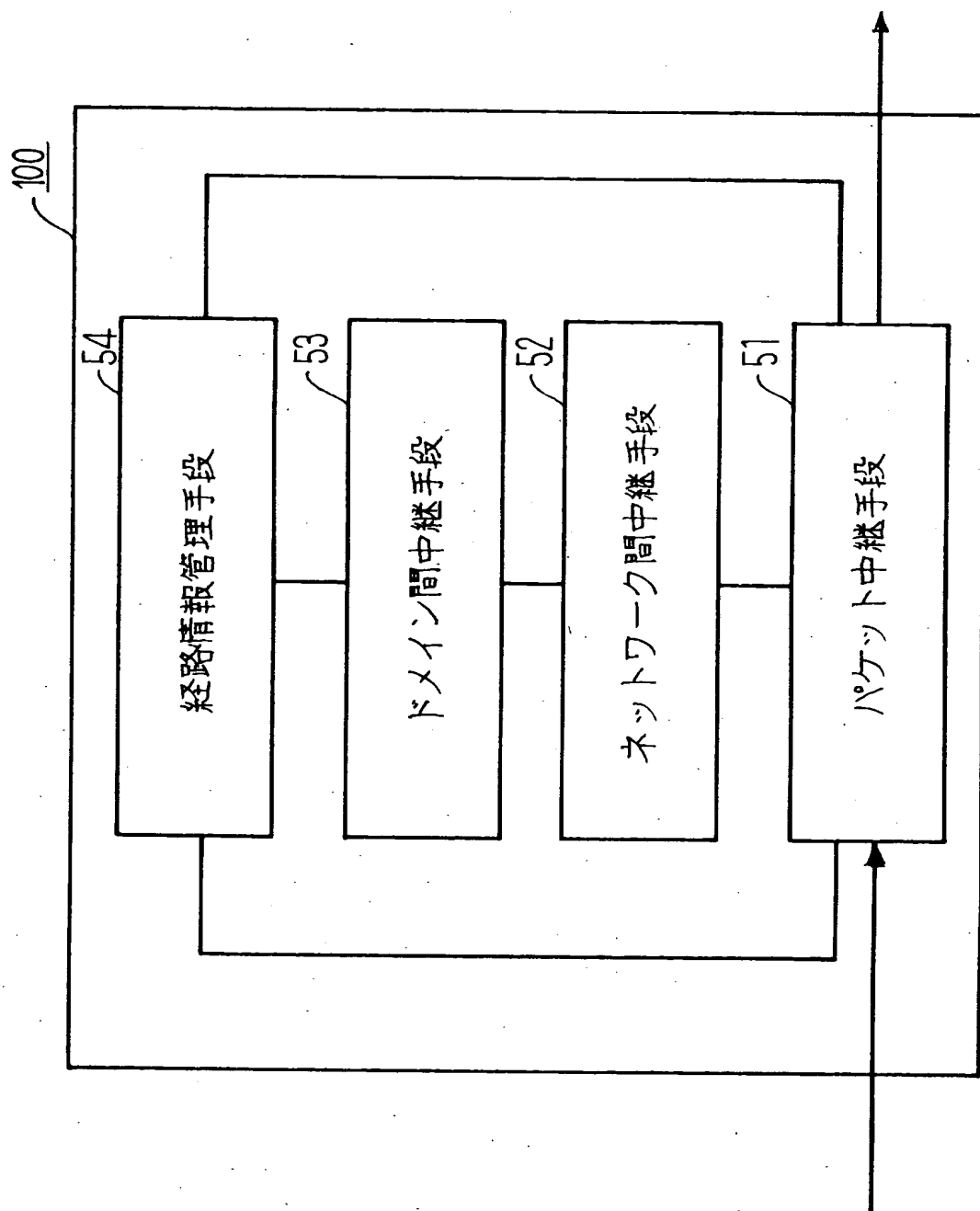
(従来技術) エキストラネットを代表するドメインに対する中継テーブルにそれぞれ重複する経路を書き込む方法



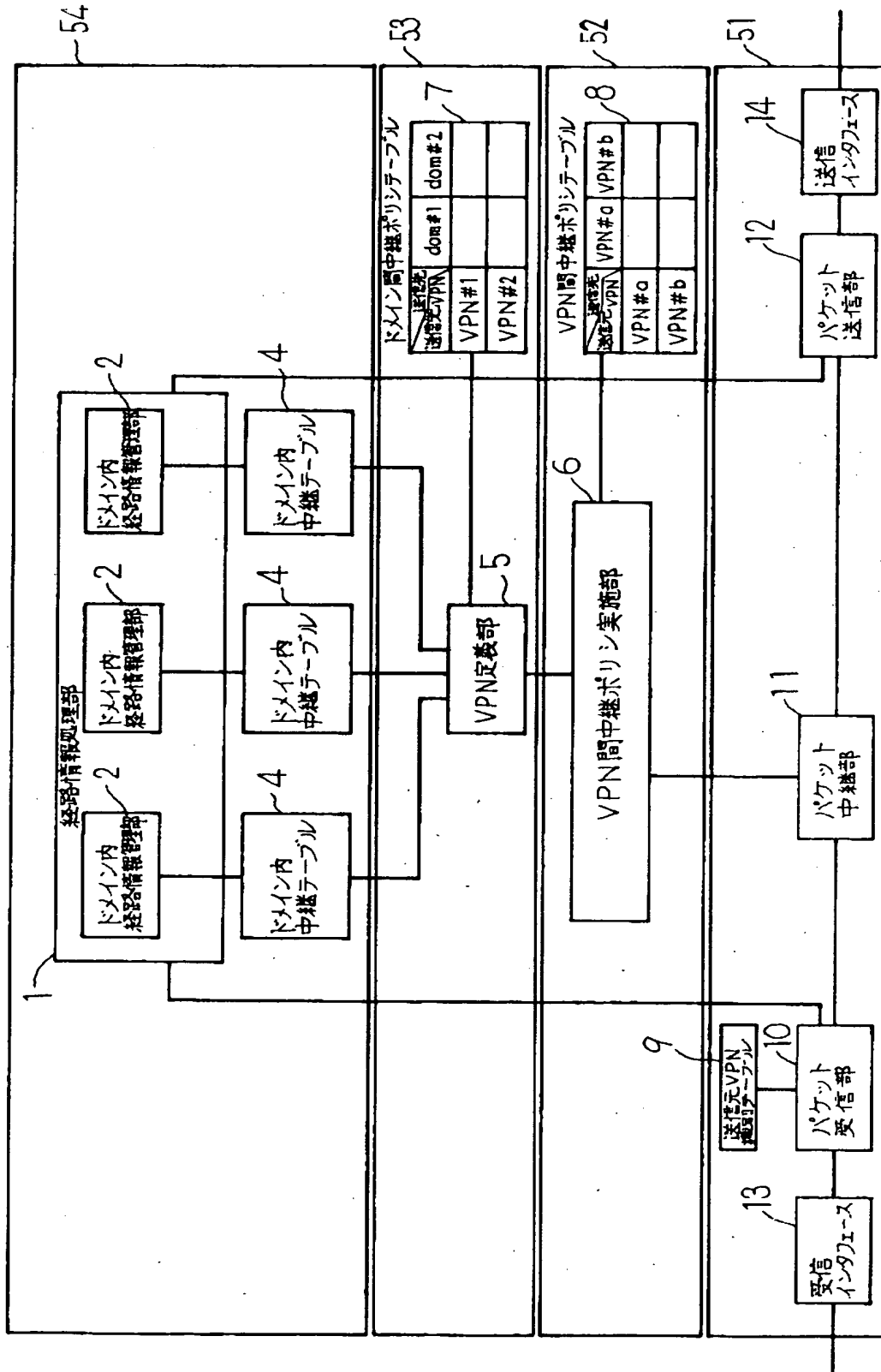
【図 3】



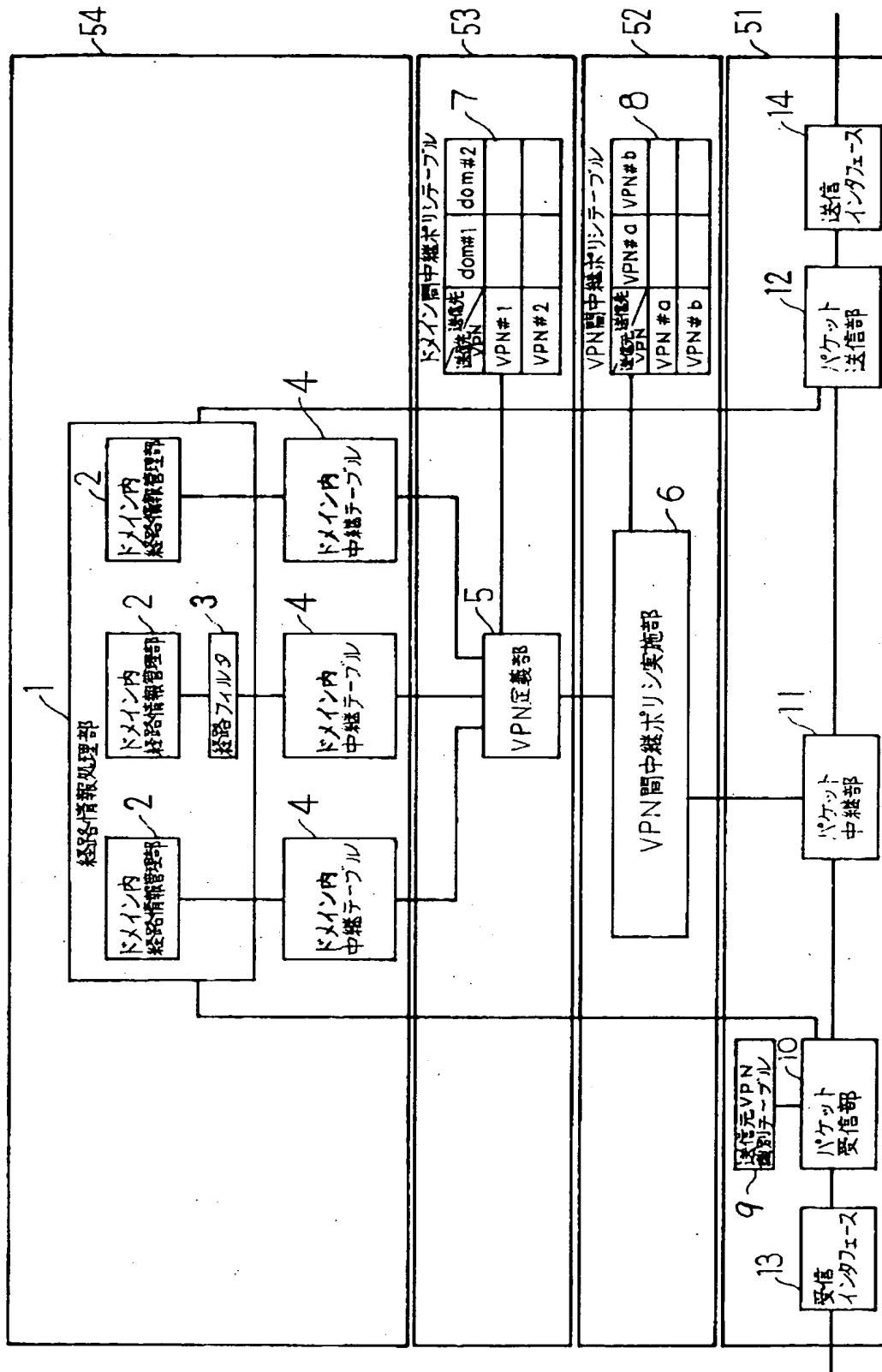
【図 4】



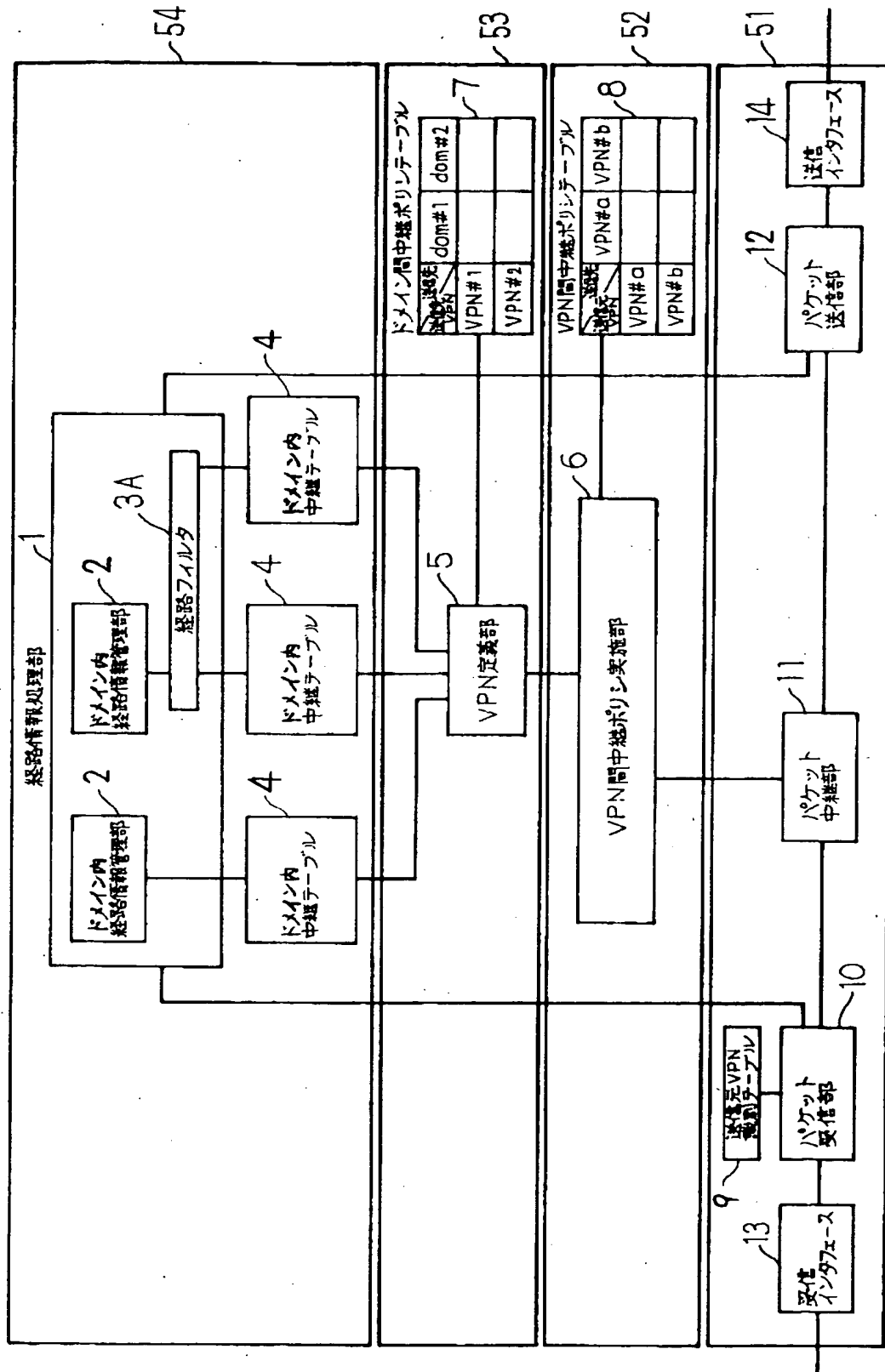
【図5】



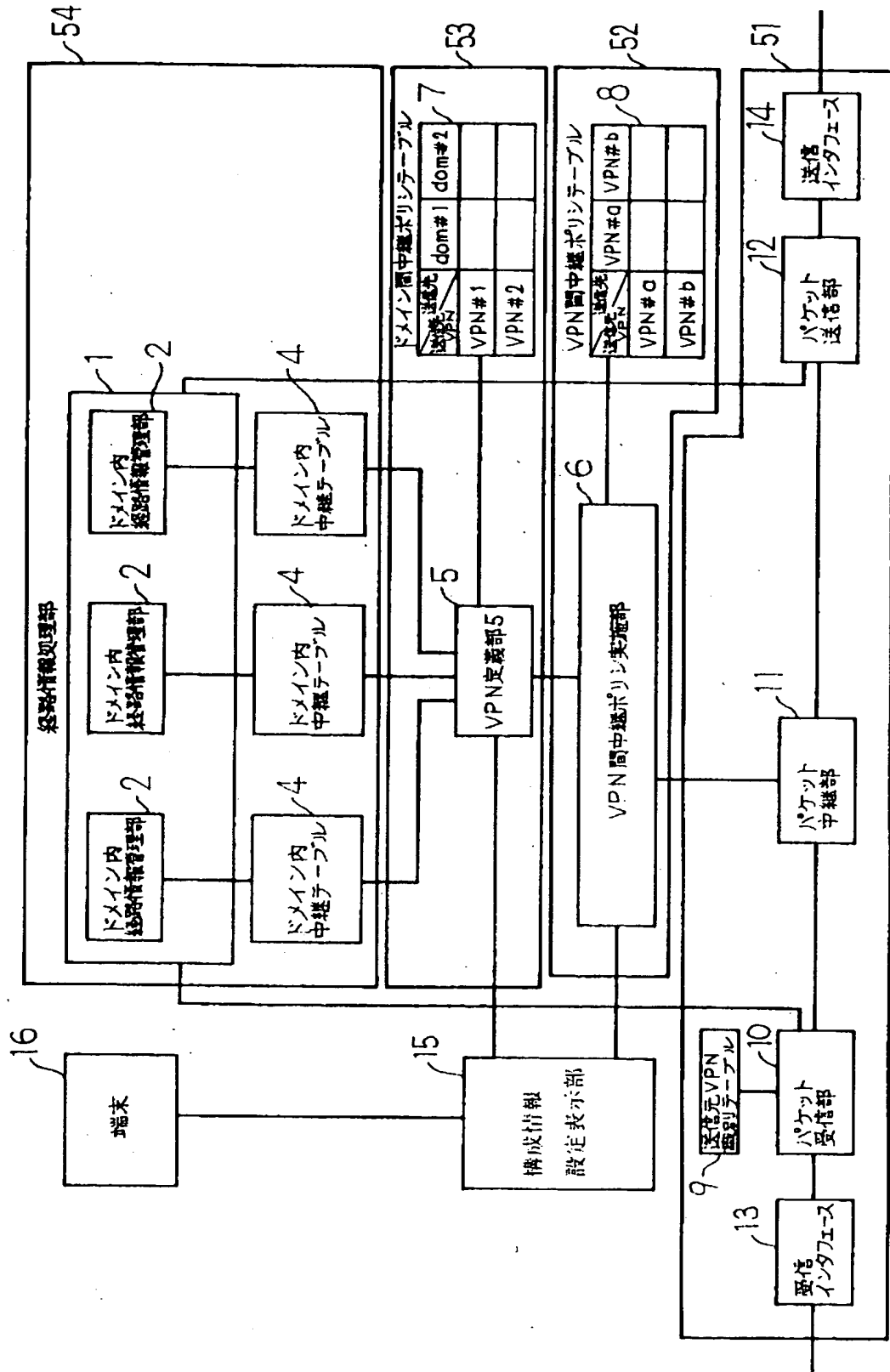
【図6】



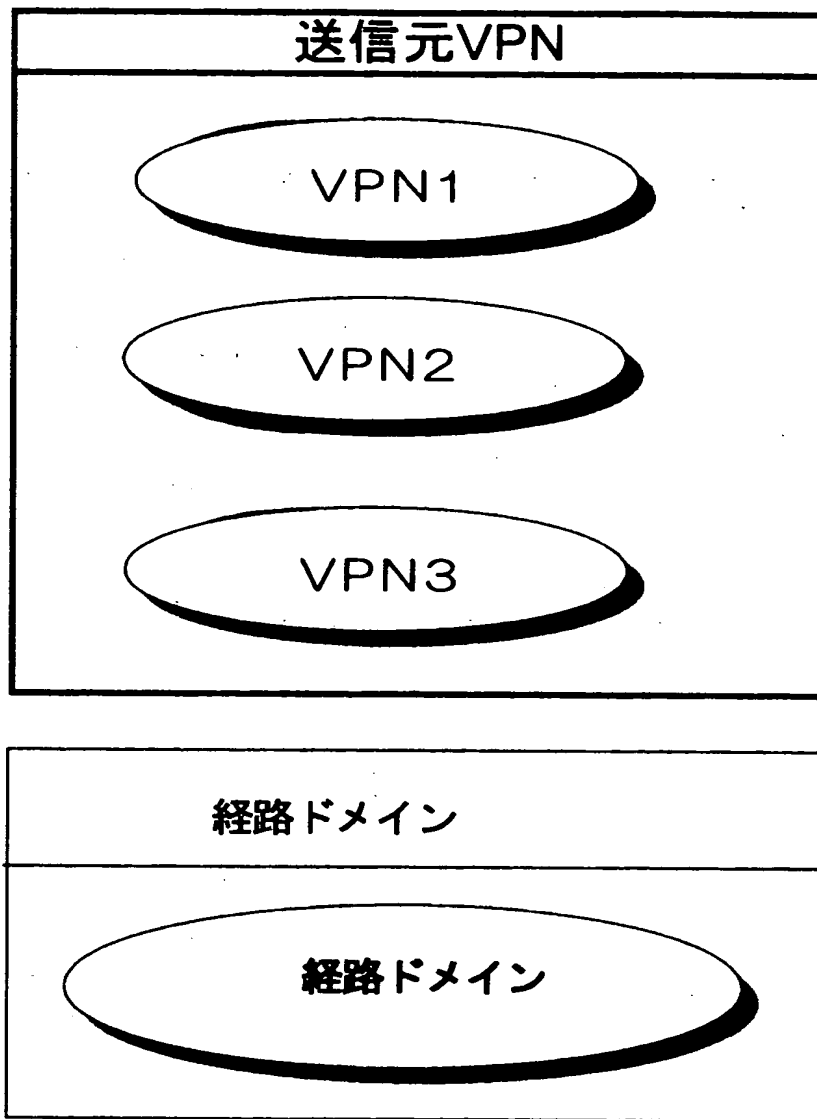
【図 7】



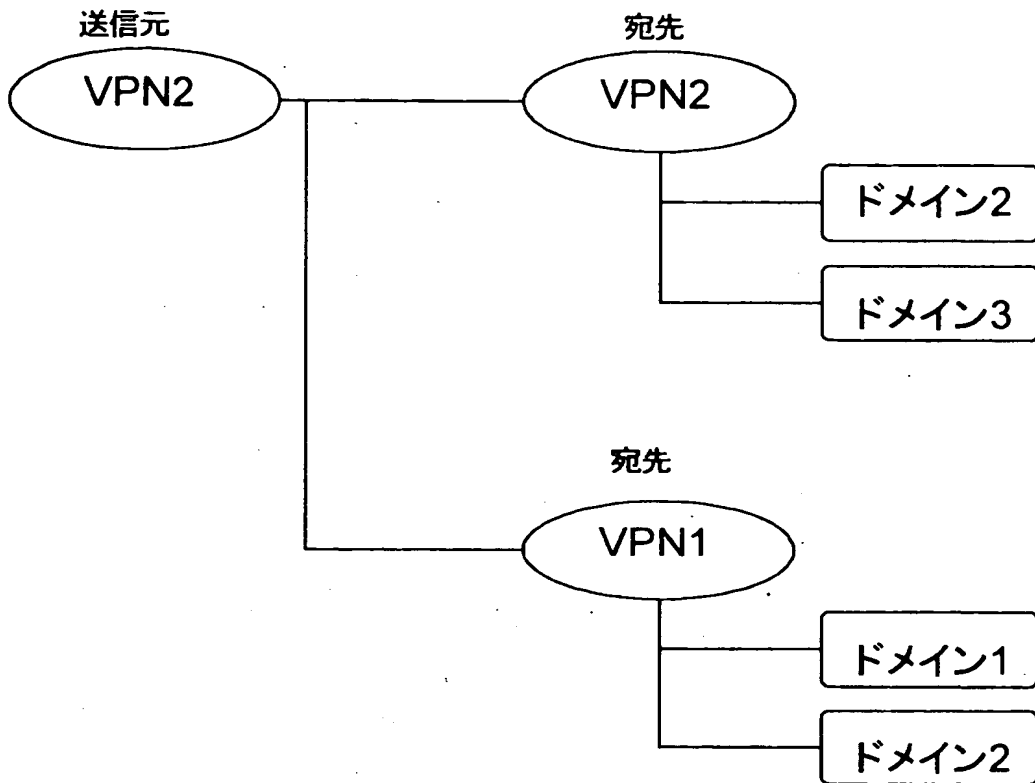
【図8】



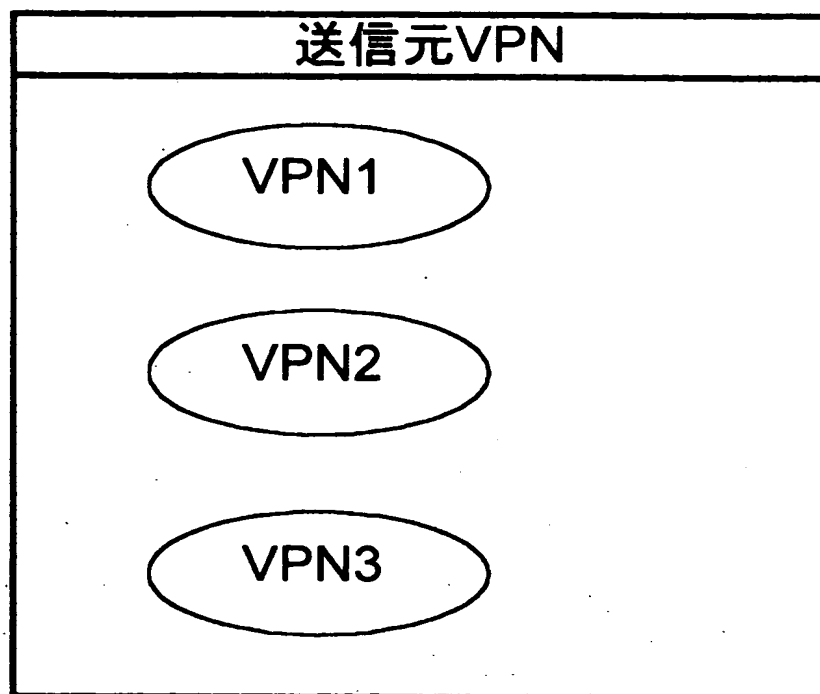
【図 9】



【図 1 0】

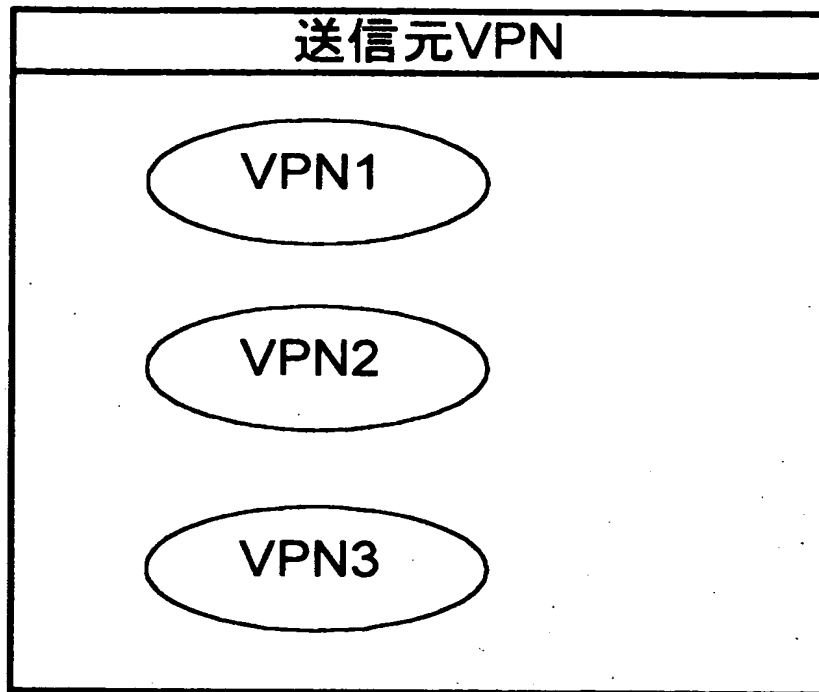


【図 11】



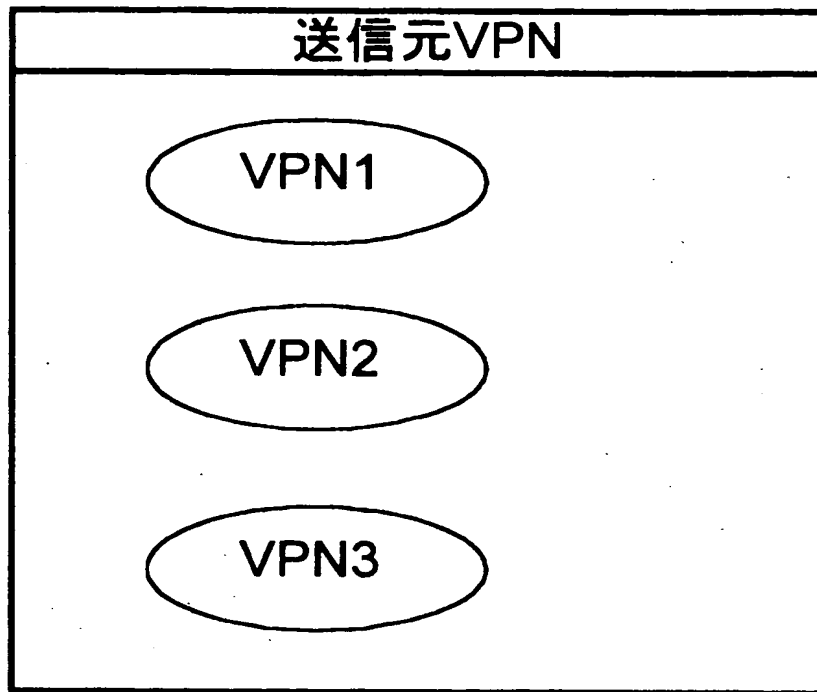
追加すべきVPN識別子=>

【図 12】



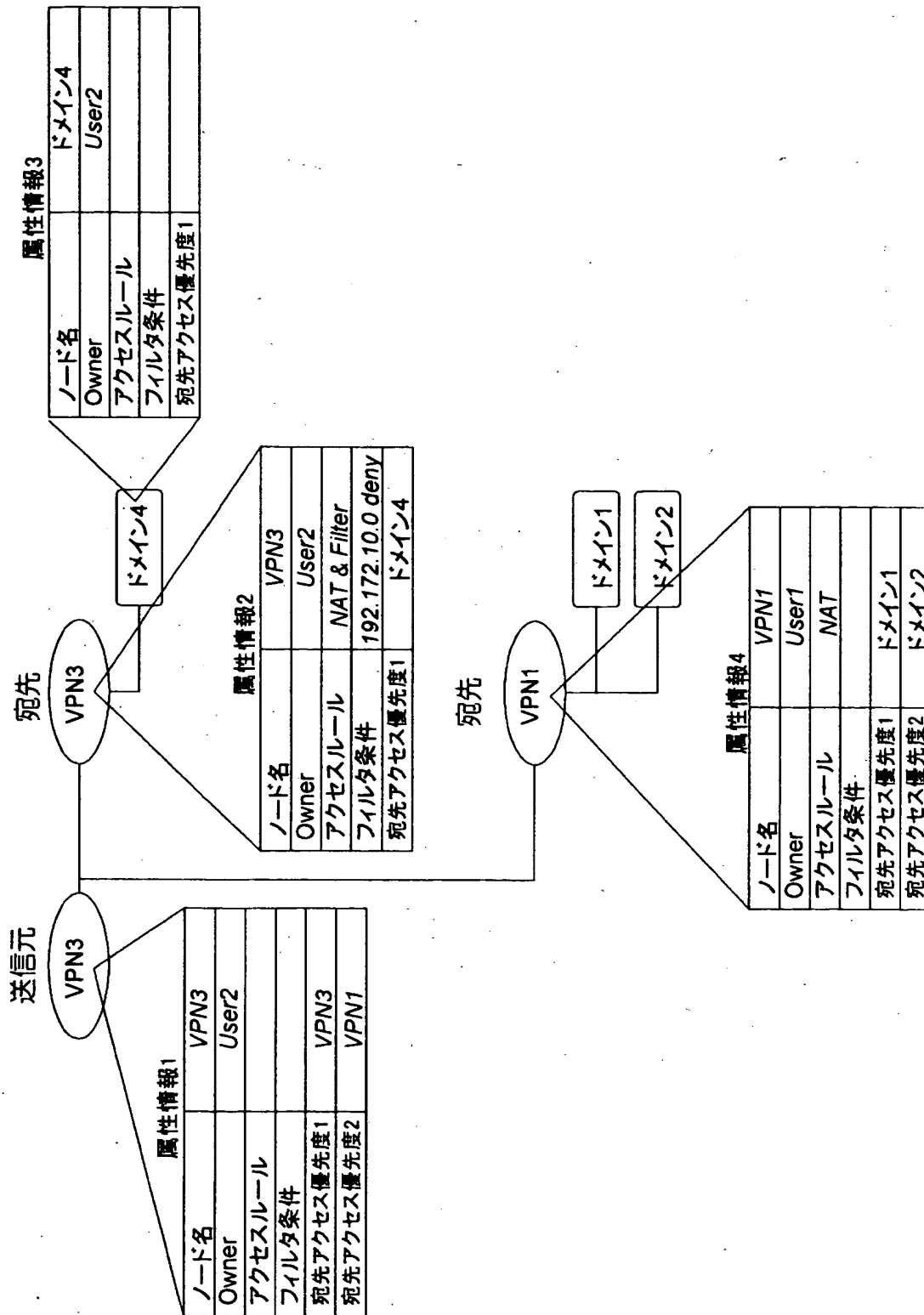
削除すべきVPN識別子==>

【図13】

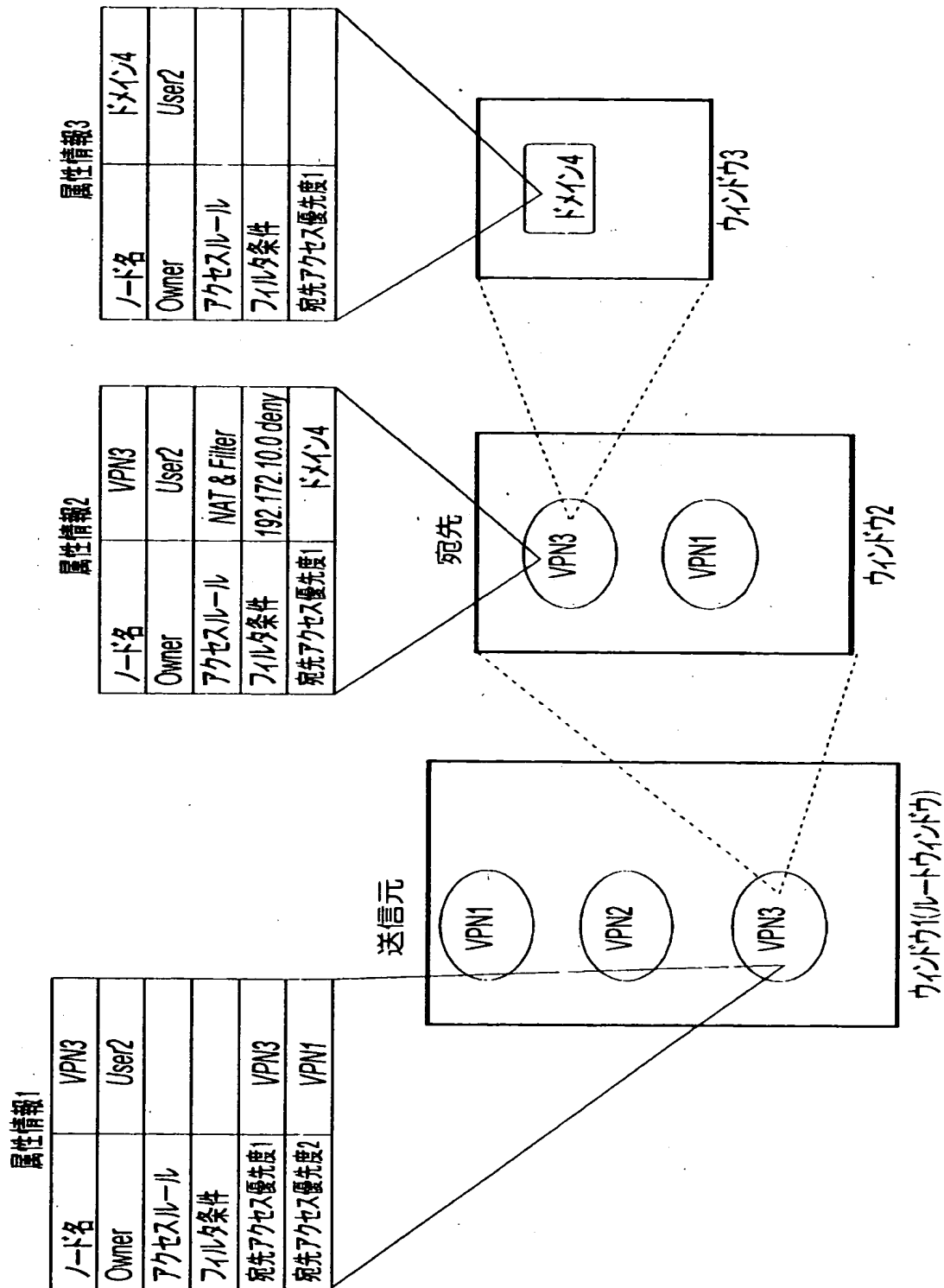


名称を変更すべきVPN識別子=>

【図 14】

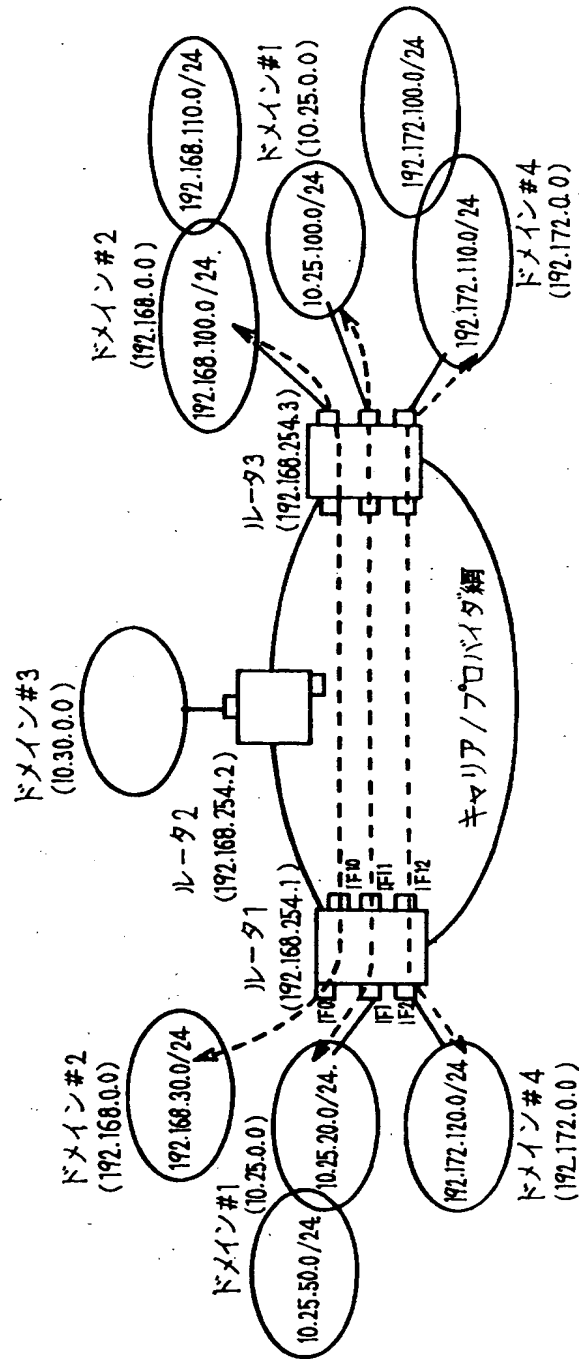


【図 15】



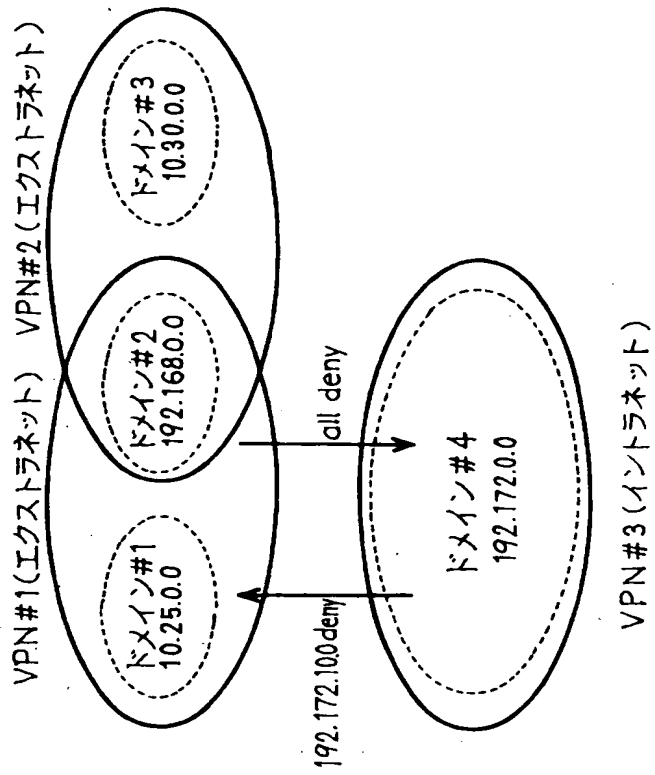
【図 16】

実施例を説明するためのネットワーク構成図



【図 1 7】

実施例を説明するためのドメイン構成図



【図18】

受信 インタフェース	送信元ドメイン	送信元VPN
IF#0	ドメイン#2	VPN#1
IF#1	ドメイン#1	VPN#1
IF#2	ドメイン#4	VPN#3

【図 19】

VPN間中継ポリシーテーブル

参照順位 受信ドメイン	1 位	2 位
VPN#1	VPN#1 permit	
VPN#2	VPN#2 permit	VPN#1 permit
VPN#3	VPN#3 permit	VPN#1 192.172.10.0 deny

【図 20】

ドメイン間中継ポリシーテーブル

参照順位 受信	1 位	2 位	...
VPN#1	ドメイン#1 permit	ドメイン#2 permit	
VPN#2	ドメイン#2 permit	ドメイン#3 permit	
VPN#3	ドメイン#4 permit		

【図 21】

ドメイン内中継テーブル(ドメイン#1)

Destination	mask	出カインタフェース	次ホップルータ
10.25.20.0	255.255.255.0	IF1	10.25.20.1
10.25.50.0	255.255.255.0	IF1	10.25.50.1
10.25.100.0	255.255.255.0	IF11	192.168.254.3

【図 22】

ドメイン内中継テーブル (ドメイン #2)

Destination	mask	出カインタフェース	次ホップルータ
192.168.30.0	255.255.255.0	IF0	192.168.30.0
192.168.100.0	255.255.255.0	IF10	192.168.254.3
192.168.110.0	255.255.255.0	IF10	192.168.254.3

【図 23】

ドメイン内中継テーブル (ドメイン #4)

Destination	mask	出カインタフェース	次ホップルータ
192.172.100.0	255.255.255.0	IF12	192.168.254.3
192.172.110.0	255.255.255.0	IF12	192.168.254.3
192.172.120.0	255.255.255.0	IF2	192.172.120.1

【書類名】 要約書

【要約】

【目的】 本発明は、パケット中継装置における中継ポリシーの設定／変更を容易にすること、また、パケット中継装置で使用されるメモリの使用量の削減することを目的とする。

【構成】 中継装置 1 0 0 において、入力されたパケットに対応する送信元ネットワーク識別子に基づき、該パケットの中継が許されている 1 つ以上のネットワークを選択するネットワーク間中継手段 5 2 と、前記 1 つ以上のネットワークに対応する 1 つ以上の経路ドメインを選択するドメイン間中継手段 5 3 と、前記パケットの送信先アドレスと前記 1 つ以上の経路ドメインの各経路ドメイン情報とを照合して前記パケットを次のパケット中継装置に送出するための次ポップルータアドレスを選択する経路情報管理手段 5 4 と、前記送出先アドレスに前記パケットを送出するパケット中継手段 5 1 とを有するように構成する。

【選択図】 図4

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号
氏 名 富士通株式会社